Installationshandbuch
Revision 1.0

VirusScan® Enterprise

Version 7.1.0



LIZENZINFORMATIONEN

Lizenzvertrag

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN FÜR SIE GELTENDEN LIZENZVERTRAG GRÜNDLICH DURCH. DIESER VERTRAG ENTHÄLT DIE ALLGEMEINEN BEDINGUNGEN UND BESTIMMUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN IHNEN NICHT BEKANNT IST, WELCHEN LIZENZTYP SIE ERWORBEN HABEN, LESEN SIE DIES IM VERKAUFSBELEG ODER IN ANDEREN ZUGEHÖRIGEN LIZENZ- ODER BESTELLDOKUMENTEN NACH, DIE SIE ZUSAMMEN MIT IHREM SOFTWARE-PAKET ODER SEPARAT IM RAHMEN DES KAUFES ERHALTEN HABEN (Z. B. EINE BROSCHÜRE, EINE DATEI AUF DER PRODUKT-CD ODER EINE DATEI AUF DER WEBSITE, AUF DER SIE DIE SOFTWARE HERUNTERGELADEN HABEN). INSTALLIEREN SIE DIE SOFTWARE NICHT, WENN SIE NICHT ALLEN IM VERTRAG ENTHALTENEN BESTIMMUNGEN ZUSTIMMEN. IN DIESEM FALL KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN NETWORK ASSOCIATES ODER DIE VERKAUFSSTELLE ZURÜCKGEBEN.

Markenhinweise

Dieses Produkt enthält möglicherweise:

- Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL-Toolkit (http://www.openssl.org/) entwickelt wurde.
- Kryptographiesoftware, die von Eric A. Young (eay@cryptsoft.com) und Software, die von Tim J. Hudson (tjh@cryptsoft.com) geschrieben wurde.
- Software-Programme, die dem Benutzer in Lizenz (oder Unterlizenz) gemäß der GNU General Public License (GPL) oder gemäß einer ähnlichen Lizenz für kostenlose Software zur Verfügung gestellt werden, wobei der Benutzer unter anderem dazu berechtigt sein kann, bestimmte Programme oder Teile davon zu kopieren, zu ändern und zu verteilen sowie auf den Quellcode zuzugreifen. Die GPL erfordert, dass für jegliche Software, die unter die GPL fällt und an eine andere Person in Form einer ausführbaren Binärdatei verteilt wird, auch der Quellcode an die entsprechende Person weitergegeben wird. Für jegliche Software, die unter die GPL fällt, steht der Quellcode auf dieser CD zur Verfügung. Wenn eine Lizenz für kostenlose Software erfordert, dass Network Associates eine Berechtigung zum Verwenden, Kopieren und Ändern eines Software-Programms gewährt, die über den Rahmen dieser Vereinbarung hinausgeht, haben diese Rechte eine höhere Priorität als die in diesem Dokument genannten Rechte und Beschränkungen.
- Software, die ursprünglich von Henry Spencer geschrieben wurde, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software, die ursprünglich von Robert Nordier geschrieben wurde, Copyright © 1996-7 Robert Nordier. Alle Rechte vorbehalten.
- Software, die von Douglas W. Sauder geschrieben wurde.
- Software, die von Apache Software Foundation (http://www.apache.org/) entwickelt wurde.
- International Components for Unicode ("ICU"), Copyright © 1995-2002 International Business Machines Corporation und andere. Alle Rechte vorbehalten.
- Software, die von der CrystalClear Software, Inc. entwickelt wurde, Copyright © 2000 CrystalClear Software, Inc.
- FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin, Deutschland.

Veröffentlicht SEPTEMBER 2003 / VirusScan® Enterprise-Software Version 7.1.0

DOKUMENTVERSION 005-DE

Inhalts

Vorwort

Dieses Handbuch enthält eine Einführung in die ® VirusScan® Enterprise-Software Version 7.1.0 von McAfee und Erläuterungen zu den folgenden Themen:

- Detaillierte Anleitungen zur Installation der Software
- Verfahrensweisen für die Änderung der Software.
- Verfahrensweisen für das Entfernen der Software.
- Informationen zur Konfigurierung des FEAD® Optimizer® von Netopsystems.
- Informationen zur Konfigurierung von Check Point™.

Zielgruppe

Die Informationen in diesem Handbuch sind in erster Linie an zwei Zielgruppen gerichtet:

- Netzwerkadministratoren, die für das Virenschutz- und Sicherheitsprogramm ihres Unternehmens verantwortlich sind.
- Benutzer, die für die Aktualisierung der Virusdefinitionsdateien (DAT-Dateien) auf ihrer Arbeitsstation oder für die Konfiguration der Erkennungsoptionen der Software verantwortlich sind.

Konventionen

In diesem Handbuch werden die folgenden Konventionen verwendet:

Fett Begriffe aus der Benutzeroberfläche, z. B. Bezeichnungen von Optionen, Menüs, Schaltflächen und Dialogfeldern

Beispiel
Geben Sie für das gewünschte Konto **Benutzername** und **Kennwort** ein.

`Courier` Vom Benutzer eingegebene Zeichenfolgen, z. B. Befehle, die an der Eingabeaufforderung des Systems eingegeben werden

Beispiel
Um den Agenten zu aktivieren, führen Sie auf dem Client-Computer die folgende Befehlszeile aus:

```
FRMINST.EXE /INSTALL=AGENT
  /SITEINFO=C:\TEMP\SITELIST.XML
```

Kursiv Betonung eines Umstands, Einführung eines neuen Begriffs, Namen der Produkthandbücher und Themenüberschriften aus diesen Handbüchern

Beispiel
Weitere Informationen finden Sie im *Produkthandbuch für VirusScan Enterprise*.

<BEGRIFF> Allgemeine Begriffe stehen in spitzen Klammern.

Beispiel
Klicken Sie in der Baumstruktur der Konsole unter **ePolicy Orchestrator** mit der rechten Maustaste auf <SERVER>.

HINWEIS Zusätzliche Informationen, z. B. eine alternative Vorgehensweise zur Ausführung eines Befehls

WARNUNG Wichtiger Hinweis zur Gewährleistung der Sicherheit des Benutzers, des Computersystems, des Unternehmens, der Softwareinstallation oder von Daten

Informationsquellen

Installationshandbuch *†	Systemanforderungen und Anweisungen zur Installation und zum Starten der Software. *VirusScan Enterprise 7.1.0 Installationshandbuch*
Produkthandbuch *	Produkteinführung und Funktionsbeschreibung, detaillierte Anweisungen zum Konfigurieren der Software, Informationen zur Bereitstellung, sich wiederholende Aufgaben und Verfahrensabläufe. *VirusScan Enterprise 7.1.0 -Produkthandbuch* *McAfee AutoUpdate Architect™ -Produkthandbuch* *McAfee Installation Designer™ -Produkthandbuch* *Warnungs-Manager™ -Produkthandbuch* *ePolicy Orchestrator™ -Produkthandbuch*
Hilfe §	Umfassende und detaillierte Informationen zu Konfiguration und Verwendung der Software *Direkthilfe* zu den einzelnen Feldern
Versionshandbuch *	Umfassende Erläuterungen zu neuen oder geänderten Funktionen der Produktversion.
Konfigurationshandbuch *	*Zur Verwendung mit ePolicy Orchestrator™*. Verfahrensweisen für die Konfiguration, Bereitstellung und Verwaltung Ihres McAfee Security-Produkts mithilfe der Verwaltungssoftware ePolicy Orchestrator.
Implementierungshandbuch *	Ergänzende Informationen zu Produktfunktionen, Tools und Komponenten
Versionshinweise ‡	*Readme*: Produktinformationen, behobene Fehler, bekannte Probleme sowie die jüngsten Ergänzungen oder Änderungen am Produkt oder der dazugehörigen Dokumentation.
Kontakt ‡	Kontaktinformationen für McAfee Security sowie für Dienstleistungen und Ressourcen von Network Associates: Technischer Support, Kundendienst, AVERT (Anti-Virus Emergency Response Team), Beta-Programm und Schulungen. Diese Datei enthält auch eine Liste der Telefon- und Faxnummern sowie Post- und Web-Adressen der Niederlassungen von Network Associates in den Vereinigten Staaten und weltweit.

* Als Adobe Acrobat-PDF-Datei auf der Produkt-CD oder der Download-Site von McAfee verfügbar.

† Als Handbuch zur Produkt-CD verfügbar. Hinweis: In einigen Sprachen stehen die Handbücher nur als PDF-Datei zur Verfügung.

‡ In der Softwareanwendung und auf der Produkt-CD enthaltene Textdateien.

§ Über die Softwareanwendung abrufbare Hilfe: Hilfemenü und/oder Hilfeschaltfläche für seitenspezifische Hilfethemen, Aufrufen der *Direkthilfe* durch Klicken mit der rechten Maustaste.

Kontaktaufnahme mit McAfee Security und Network Associates

Technischer Support	
Homepage	http://www.networkassociates.com/us/support/
KnowledgeBase-Zugang	https://knowledgemap.nai.com/phpclient/homepage.aspx
Service-Portal für PrimeSupport*	http://mysupport.nai.com
Beta-Programm für McAfee Security	http://www.networkassociates.com/us/downloads/beta/
Security-Zentrale – AVERT (Anti-Virus Emergency Response Team)	
Homepage	http://www.networkassociates.com/us/security/home.asp
Virusinformationsbibliothek	http://vil.nai.com
Einsenden von Beispielen – AVERT WebImmune	https://www.webimmune.net/default.asp
AVERT DAT-Benachrichtigungsdienst	http://www.networkassociates.com/us/downloads/updates/
Download-Site	
Homepage	http://www.networkassociates.com/us/downloads/
DAT-Datei- und Modul-Aktualisierungen	http://www.networkassociates.com/us/downloads/updates/
	ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
Produkt-Upgrades*	https://secure.nai.com/us/forms/downloads/upgrades/login.asp
Schulungen	
McAfee Security University	http://www.networkassociates.com/us/services/education/mcafee/university.htm
Network Associates-Kundendienst	
E-Mail	services_corporate_division@nai.com
Web	http://www.nai.com/us/index.asp
	http://www.networkassociates.com/us/products/mcafee_security_home.htm
USA, Kanada und Lateinamerika (gebührenfrei):	
Telefon:	**+1-888-VIRUS NO** oder **+1-888-847-8766**
	Mo – Fr, 08:00 – 20:00 Uhr, Central Time
Weitere Informationen zur Kontaktaufnahme mit Network Associates und McAfee Security (einschließlich gebührenfreier Nummern für andere Länder) finden Sie in der Kontakt-Datei, die im Lieferumfang dieses Produkts enthalten ist.	

* Anmeldedaten müssen eingegeben werden.

Installieren der Software 1

Die Software VirusScan Enterprise 7.1.0 unterstützt sowohl Server als auch Arbeitsstationen sowie eine Vielzahl von Anwendungen anderer Hersteller. Das Programm ersetzt folgende Softwareversionen:

- VirusScan Enterprise Version 7.0 für Arbeitsstationen und Server.
- VirusScan Version 4.5.1 für Arbeitsstationen.
- NetShieldNT Version 4.5 für Server.
- NetShield for Celerra™ Version™ 4.5 für Celerra-Dateiserver.

Diese Themen sind in diesem Abschnitt enthalten:

Vorbereitung

Um die Installation vorzubereiten, lesen Sie vor dem Start bitte folgende Punkte:

- *Installationsvorbereitende Verfahren* auf Seite 10.
- *Systemanforderungen* auf Seite 11.
- *Bereitstellungs-, Aktualisierungs- und Verwaltungsoptionen* auf Seite 13.
- *Installation und Konfiguration für den Einsatz mit anderen Produkten* auf Seite 15.
- *Produktlizenz* auf Seite 16.

Installationsvorbereitende Verfahren

Führen Sie, bevor Sie mit der Installation beginnen, diese Verfahren vollständig durch:

- **Produktsoftware** – Suchen Sie die VirusScan Enterprise 7.1.0-Software.

  McAfee Security vertreibt die VirusScan Enterprise-Software auf zwei Arten:

  - Als Archivdatei, die aus dem Internet heruntergeladen werden kann. Rufen Sie die Download-Website von McAfee Security auf, um die Archivdatei herunterzuladen. Siehe *Kontaktaufnahme mit McAfee Security und Network Associates* auf Seite 8.
  - Auf einer Produkt-CD.

- **Readme** – Suchen Sie die *Readme*-Datei und lesen Sie den Inhalt gründlich durch. Sie enthält besondere Installationsanweisungen oder Hinweise zu Problemen. Die *Readme*-Datei befindet sich in demselben Verzeichnis wie die Produktsoftware.

- **Installationsberechtigung** – Vergewissern Sie sich, dass Sie über die erforderlichen Rechte für die Installation der Software verfügen. Um VirusScan Enterprise installieren zu können, müssen Sie auf dem Computer, auf dem Sie das Programm installieren möchten, über Administratorrechte verfügen.

- **Einstellungen beibehalten** – Legen Sie, wenn Sie eine ältere Version der Software aktualisieren, fest, ob die bestehenden Einstellungen beibehalten werden sollen.

  Wenn Sie VirusScan Enterprise 7.1.0 auf einem Computer mit einer älteren Version von NetShield VirusScan oder VirusScan Enterprise installieren, steht Ihnen die Option zur Verfügung, die Einstellungen der älteren Software zu übernehmen. Wenn Sie Einstellungen beibehalten, werden gespeicherte Tasks, benutzerdefinierte Dateierweiterungen und Ausschlüsse der zuvor installierten Software gespeichert.

  Alternativ können Sie die vorherige Version entfernen und anschließend VirusScan Enterprise 7.1.0 installieren. Bei dieser Verfahrensweise gehen die für die vorherige Softwareversion festgelegten Einstellungen verloren.

Systemanforderungen

Bevor Sie mit der Installation beginnen, prüfen Sie, ob der Computer folgende Systemanforderungen erfüllt.

Serveranforderungen

VirusScan Enterprise kann auf Servern installiert und ausgeführt werden, die die folgenden Anforderungen erfüllen:

- **Prozessor** – Intel-Prozessor oder kompatible Architektur. McAfee Security empfiehlt einen Intel Pentium- oder Celeron-Prozessor mit mindestens 166 MHz.
- **Betriebssystem** – Eine der folgenden Microsoft Windows-Plattformen:
  - Windows NT Server 4.0 mit Service Pack 6 oder 6a.
  - Windows NT Enterprise Server 4.0 mit Service Pack 6 oder 6a.
  - Windows NT Terminal Server Edition mit Service Pack 6.
  - Windows 2000 Server mit Service Pack 1, 2 oder 3.
  - Windows 2000 Advanced Server mit Service Pack 1, 2 oder 3.
  - Windows 2000 DataCenter Server mit Service Pack 1, 2 oder 3.
  - Windows Server 2003 Standard (früher Windows .NET Server 2003, Standard Edition).
  - Windows Server 2003 Enterprise (früher Windows .NET Server 2003, Enterprise Edition).
  - Windows Server 2003 Web (früher Windows .NET Server 2003, Web Edition).
  - Windows Server 2003 DataCenter.
- **Browser** – Microsoft Internet Explorer Version 4.0 oder höher.
- **Hauptspeicher** – mindestens 32 MB RAM.

HINWEIS
Informationen über die optimale Betriebssystemleistung finden Sie in den Microsoft-Richtlinien für RAM-Mindestanforderungen.

- **Freier Festplattenspeicher** – Entsprechender Festplattenspeicher:
  - **20** MB **–** Eine vollständige Installation aller Programmfeatures und -komponenten benötigt auf dem Computer etwa 20 MB Festplattenspeicher.
  - **25** MB **–** Für die Installation werden zusätzliche 25 MB als temporärer Speicher verwendet, der nach Abschluss der Installation wieder freigegeben wird.
- **Sonstiges** – Ein CD-ROM-Laufwerk oder eine Internet-Verbindung.

Anforderungen an Arbeitsstationen

VirusScan Enterprise kann auf jeder Arbeitsstation installiert und ausgeführt werden, die folgende Anforderungen erfüllt:

- **Prozessor** – Intel-Prozessor oder kompatible Architektur. McAfee Security empfiehlt einen Intel Pentium- oder Celeron-Prozessor mit mindestens 166 MHz.
- **Betriebssystem** – Eine der folgenden Microsoft Windows-Plattformen:
  - Windows NT Workstation 4.0 mit Service Pack 6 oder 6a.
  - Windows 2000 Professional mit Service Pack 1, 2 oder 3.
  - Windows XP Home, Professional und Tablet PC Edition mit Service Pack 1.
- **Browser** – Microsoft Internet Explorer Version 4.0 oder höher.
- **Hauptspeicher** – mindestens 32 MB RAM.

  HINWEIS
  Informationen über die optimale Betriebssystemleistung finden Sie in den Microsoft-Richtlinien für RAM-Mindestanforderungen.

- **Freier Festplattenspeicher** – Entsprechender Festplattenspeicher:
  - **20** MB **–** Eine vollständige Installation aller Programmfeatures und -komponenten benötigt auf dem Computer etwa 20 MB Festplattenspeicher.
  - **25** MB **–** Für die Installation werden zusätzliche 25 MB als temporärer Speicher verwendet, der nach Abschluss der Installation wieder freigegeben wird.
- **Sonstiges** – Ein CD-ROM-Laufwerk oder eine Internet-Verbindung.

Bereitstellungs-, Aktualisierungs- und Verwaltungsoptionen

Legen Sie fest, wie das Produkt bereitgestellt, verwaltet und aktualisiert werden soll. Wenn Sie vorhaben, Unterstützungstools für die Bereitstellung, Vorkonfigurierung, Aktualisierung oder Verwaltung von VirusScan Enterprise zu verwenden, kann das Installationsverfahren abweichen.

Beim Vorkonfigurieren des Installationspakets von VirusScan Enterprise sollte Folgendes beachtet werden:

- Woher und wie Aktualisierungen bezogen werden.
- Wann nach Aktualisierungen gesucht wird (die Standardeinstellung ist Freitag, 17:00 Uhr Ortszeit des Computers).
- Welche Richtlinieneinstellungen definiert werden sollen.

Vorkonfigurieren des Installationspakets

Gehen Sie wie folgt vor, um das VirusScan Enterprise-Installationspaket vorzukonfigurieren:

- *Mit MacAfee AutoUpdate Architect und McAfee Installation Designer* auf Seite 13.
- *Verwenden von ePolicy Orchestrator* auf Seite 14.

Mit MacAfee AutoUpdate Architect und McAfee Installation Designer

Um das Installationspaket mit McAfee AutoUpdate Architect und McAfee Installation Designer vorzukonfigurieren, gehen Sie wie folgt vor:

HINWEIS
Wenn Sie die FTP- oder HTTP-Aktualisierungs-Sites von Network Associates als Aktualisierungsort verwenden wollen, überspringen Sie Schritt 1 und Schritt 2. Die VirusScan Enterprise-Software ist bereits so vorkonfiguriert, dass Aktualisierungen von diesen Standardspeicherorten abgerufen werden. Standardspeicherort ist die FTP-Site. Die HTTP-Site ist in der Repository-Liste als nächster Speicherort vorgegeben.

Weitere Informationen zur Aktualisierung oder Verwendung der FTP- bzw. HTTP-Aktualisierungs-Sites von Network Associates finden Sie im *VirusScan Enterprise 7.1.0-Produkthandbuch*.

1 Installieren Sie McAfee AutoUpdate Architect und konfigurieren Sie damit die VirusScan Enterprise-Repository-Liste SITELIST.XML. Weitere Informationen finden Sie im *Produkthandbuch des McAfee AutoUpdate Architect*. Die Repository-Liste enthält die verfügbaren Aktualisierungs-Sites, die VirusScan Enterprise für die Aktualisierung verwendet.

2 Exportieren Sie die Repository-Liste, SITELIST.XML, in einen temporären Ordner.

3 Installieren Sie McAfee Installation Designer und verwenden Sie dieses Programm zur Anpassung der Installationsoptionen für VirusScan Enterprise 7.1.0. Weitere Informationen finden Sie im *Produkthandbuch für McAfee Installation Designer*.

Verwenden von ePolicy Orchestrator

Wenn Sie ePolicy Orchestrator vor der Bereitstellung von VirusScan Enterprise 7.1.0 installiert haben, können Sie ePolicy Orchestrator zum Vorkonfigurieren der Richtlinieneinstellungen und zum Aktualisieren der Konfiguration benutzen. Weitere Informationen finden Sie im *VirusScan Enterprise-Konfigurationshandbuch zur Verwendung mit ePolicy Orchestrator*.

HINWEIS
Bevor Sie den ePolicy Orchestrator verwenden, um die Software auf die Client-Computer zu laden, sollten Sie mithilfe von McAfee Installation Designer die im Installationspaket enthaltenen Standard-Virusdefinitionsdateien (DAT) und die Moduldateien ersetzen. Dies gewährleistet, dass der Client-Computer zum Zeitpunkt der Installation über den aktuellsten Schutz verfügt. Außerdem wird so weniger Netzwerk-Bandbreite benötigt, da die aktualisierten Dateien nach der Installation nicht abgerufen werden müssen.

Welche Optionen Ihnen zur Verfügung stehen, hängt davon ab, welche Version von ePolicy Orchestrator Sie verwenden.

Bei Verwendung von ePolicy Orchestrator 3.0

ePolicy Orchestrator Version 3.0 oder höher beinhaltet McAfee AutoUpdate Architect. Mit diesem Programm können Sie Ihre Aktualisierungs-Repositories erstellen und verwalten. Dadurch wird gewährleistet, dass die Produktinstallationen und Aktualisierungen aus einer lokalen Quelle erfolgen. Weitere Informationen finden Sie im *Produkthandbuch des McAfee AutoUpdate Architect*.

Mit dem ePolicy Orchestrator 3.0 können Sie die Richtlinien und Aktualisierungen von VirusScan Enterprise problemlos festlegen und ändern. Weitere Informationen finden Sie im *VirusScan Enterprise-Konfigurationshandbuch zur Verwendung mit ePolicy Orchestrator 3.0*.

Bei der Verwendung von ePolicy Orchestrator 3.0 sollten Sie den in ePolicy Orchestrator enthaltenen McAfee AutoUpdate Architect verwenden, um vor dem Bereitstellen von VirusScan Enterprise 7.1.0 die Repositories zu erstellen.

Bei Verwendung von ePolicy Orchestrator 2.5.x

ePolicy Orchestrator Version 2.5.x kann VirusScan Enterprise-Richtlinien verwalten. ePolicy Orchestrator 2.5.x beinhaltet jedoch nicht McAfee AutoUpdate Architect. Daher müssen Sie für die Erstellung und Verwaltung Ihrer Aktualisierungs-Repositories eine Standalone-Version von McAfee AutoUpdate Architect verwenden. Um die erstellten Repository-Sites verwenden zu können, müssen Sie zunächst in ePolicy Orchestrator 2.5.x die AutoUpdate-Tasks für VirusScan Enterprise definieren. Weitere Informationen finden Sie im *VirusScan Enterprise-Konfigurationshandbuch zur Verwendung mit ePolicy Orchestrator 2.5.x*.

Installation und Konfiguration für den Einsatz mit anderen Produkten

Wenn Sie die VirusScan Enterprise-Software zusammen mit anderen Produkten installieren oder den Einsatz von VirusScan Enterprise mit unterstützenden Produkten planen, kann es notwendig sein, dass Sie das Installationsverfahren verändern oder zusätzliche Konfigurationen vornehmen müssen.

Diese Themen sind in diesem Abschnitt enthalten:

Netopsystems FEAD Optimizer

Die Installationsdatei für VirusScan Enterprise 7.1.0 (.MSI) wurde mithilfe der Fast Electronic Application Distribution-Technologie (FEAD® Optimizer®) von Netopsystems optimiert. Dadurch wird die Größe der Installationsdatei bis zu ihrem Neuaufbau erheblich reduziert.

Wenn Sie das Setup-Dienstprogramm für die Installation der VirusScan Enterprise-Software verwenden, wird diese Datei vor Beginn der Installation automatisch neu aufgebaut.

Wenn Sie SETUP.EXE über die Befehlszeile ausführen, können Sie spezielle Befehlszeileneinstellungen und Optionen anwenden, um die Installationsdateien neu aufzubauen. Weitere Informationen finden Sie unter *Netopsystems FEAD Optimizer* auf Seite 61.

Sie können die Installationsdatei mithilfe von McAfee Installation Designer neu aufbauen und sie dann nach der Vornahme von Änderungen erneut optimieren. Weitere Informationen finden Sie im *Produkthandbuch für McAfee Installation Designer*.

Windows Terminal Server

Wenn die Windows NT Terminal Server Edition oder Windows 2000 oder 2003 Terminal Server Application installiert ist und Sie für die Installation der VirusScan Enterprise-Software das Setupprogramm verwenden, wird die Installation angehalten und der Benutzer benachrichtigt, dass er das Produkt über die Windows-Systemsteuerung mithilfe des Dienstprogramms "Software" installieren muss.

Um das Dienstprogramms "Software" aufzurufen, klicken Sie auf **Start**, wählen Sie dann **Einstellungen** | **Systemsteuerung** | **Software**.

> **HINWEIS**
> Dieses Installationsverfahren ist nicht notwendig, wenn Sie VirusScan Enterprise mit dem ePolicy Orchestrator bereitstellen.

EMC Celerra-Server

Wenn Sie die VirusScan Enterprise-Software auf einem EMC Celerra-Server installieren möchten, müssen Sie zuerst die EMC Scanner Server-Software und erst danach die VirusScan Enterprise 7.1.0-Software installieren. Dadurch wird gewährleistet, dass die VirusScan Enterprise-Software ordnungsgemäß mit den Einstellungen des EMC Celerra-Servers konfiguriert wird.

Check Point

Die VirusScan Enterprise-Software wurde hinsichtlich der Integration von Check Point™ VPN-1/FireWall-1® SCVerweitert. Diese Integration versetzt Sie in die Lage, zu verhindern, dass Clients ohne aktuellen Virenschutz über das Virtual Private Network (VPN) in das Firmennetz gelangen. Weitere Informationen dazu finden Sie unter *Check Point konfigurieren* auf Seite 63.

Produktlizenz

Bei der Erstinstallation einer lizenzierten Version von VirusScan Enterprise 7.1.0 wird das Produkt während der Installation lizenziert. Überspringen Sie diesen Abschnitt, und lesen Sie *Installieren von VirusScan Enterprise* auf Seite 17.

Wenn Sie eine lizenzierte Version der VirusScan Enterprise 7.1.0-Software über eine Testversion installieren, müssen Sie die Testversion auf eine lizenzierte Version aktualisieren. Die Lizenz wird nicht automatisch aktualisiert, wenn Sie eine Installation über eine bestehende Testversion durchführen.

WARNUNG
Die Lizenz muss vor Ablauf der Testfrist aktualisiert werden. Bei Überschreiten der Frist werden Scan- und Aktualisierungsfunktionen gestoppt und können erst wieder ausgeführt werden, nachdem die Testversion durch die lizenzierte Version des Produkts ersetzt wurde.

Um eine Testversion von VirusScan Enterprise durch die lizenzierte Version zu ersetzen, können Sie nach einer der folgenden Verfahrensweisen vorgehen:

- Verwenden Sie zur Aktualisierung der installierten Testversion auf eine lizenzierte Version McAfee Installation Designer. Gehen Sie dabei folgendermaßen vor:
  - Installieren Sie die lizenzierte Version von VirusScan Enterprise.
  - Verwenden Sie McAfee Installation Designer, um die Lizenz zu aktualisieren. Einzelheiten zu diesem Vorgang finden Sie im *Produkthandbuch für McAfee Installation Designer.*
- Entfernen Sie die vorhandene Testversion des Produkts, und installieren Sie die lizenzierte Version des Produkts. Wenn Sie nach dieser Verfahrensweise vorgehen, gehen die für die vorherige Installation festgelegten Einstellungen verloren. Die Verfahrensweise empfiehlt sich daher nur, wenn McAfee Installation Designer zum Aktualisieren der Lizenz nicht verwendet werden kann.

Installieren von VirusScan Enterprise

Sie können die VirusScan Enterprise-Programmdateien entweder auf einem Server oder einer Arbeitsstation installieren.

HINWEIS
Das Installationsprogramm ermittelt, ob die Installation auf einem Server oder auf einer Arbeitsstation erfolgt, und stellt einen Registrierungswert für das Reporting von ePolicy Orchestrator (über Plugin) an den *McAfeeVirusScan Enterprise-Server* oder an die *VirusScan Enterprise-Arbeitsstation* ein.

Auf diese Weise kann ePolicy Orchestrator beim Reporting und bei der Durchsetzung von Richtlinien zwischen einem Server und einer Arbeitsstation unterscheiden.

Verwenden Sie eine der folgenden Methoden, um VirusScan Enterprise zu installieren:

- Das Setup-Dienstprogramm, das in VirusScan Enterprise integriert ist.
- Die Befehlszeile.
- Mit McAfee Installation Designer können Sie ein angepasstes Installationspaket erstellen und Produkteinstellungen konfigurieren. Ausführliche Anweisungen finden Sie im *Produkthandbuch für McAfee Installation Designer*.

Bevor Sie mit der Installation beginnen, lesen Sie die *Systemanforderungen* auf Seite 11.

Diese Themen sind in diesem Abschnitt enthalten:

Verwenden des Setupprogramms

Auf dem Computer, auf dem das Programm installiert werden soll:

1 Öffnen Sie das Dialogfeld **McAfee VirusScan Enterprise-Setup** mit einer der folgenden Methoden:

   Wenn sich Ihre Kopie der Software auf der Produkt-CD befindet:

   a Legen Sie die CD in das CD-ROM-Laufwerk ein.

   b Klicken Sie im Dialogfeld **Willkommen** auf **Installation**.

   Wenn Sie die Software herunterladen:

   a Erstellen Sie einen temporären Ordner auf der Festplatte.

   b Laden Sie die Archivdatei von der McAfee Security-Download-Website herunter. Siehe *Kontaktaufnahme mit McAfee Security und Network Associates* auf Seite 8.

c Extrahieren Sie die in diesen Ordner heruntergeladenen Dateien mithilfe eines Entkomprimierungsprogramms (z. B. WinZip).

d Klicken Sie auf **Start**, und wählen Sie anschließend **Ausführen**. Das Dialogfeld **Ausführen** wird angezeigt.

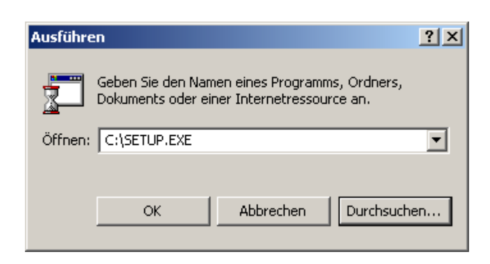


Abbildung 1-1. Ausführen

e Geben Sie in das Textfeld den Befehl <X>:\SETUP.EXE ein, und klicken Sie auf **OK**.

<X>: steht dabei für den Laufwerksbuchstaben des CD-ROM-Laufwerks bzw. für den Pfad zu dem Ordner, der die entpackten Programmdateien enthält. Um nach der entsprechenden Datei auf der Festplatte oder CD-ROM zu suchen, klicken Sie auf **Durchsuchen**. Wenn Sie die Software von einer Produktsuite-CD installieren, müssen Sie außerdem angeben, in welchem Ordner die gewünschte Software gespeichert ist.

Das Dialogfeld **Netopsystems FEAD Optimizer** wird geöffnet.

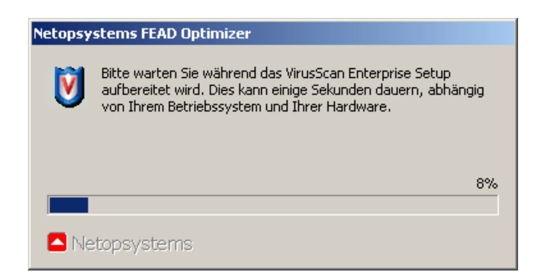


Abbildung 1-2. Netopsystems FEAD Optimizer

HINWEIS
Es kann ein paar Minuten dauern, bis die Dateien neu aufgebaut sind. Das nächste Dialogfeld wird angezeigt, nachdem die Dateien neu aufgebaut wurden.

Das Dialogfeld **McAfee VirusScan Enterprise-Setup** wird angezeigt.



Abbildung 1-3. McAfee VirusScan Enterprise-Setup

2 Lesen Sie die Produktinformationen:

a Klicken Sie auf **Readme anzeigen**, um die README-Datei anzuzeigen. Klicken Sie dann auf **OK**, um wieder zum Dialogfeld **McAfee VirusScan Enterprise-Setup** zurückzukehren.

b Wenn Sie die Produktinformationen gelesen haben, klicken Sie auf **Weiter**, um das Dialogfeld für die **Network Associates-Lizenzierung** zu öffnen.

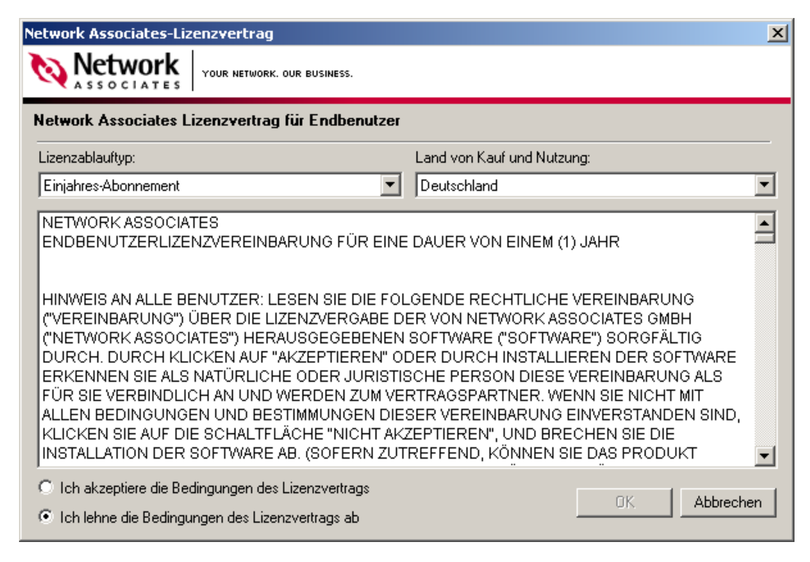


Abbildung 1-4. Network Associates-Lizenz

3 Klicken Sie im Textfeld für den **Lizenzablauftyp** auf ▾, um den Lizenztyp auszuwählen.

> **HINWEIS**
> Der Gültigkeitszeitraum des Lizenztyps muss mit dem Zeitraum übereinstimmen, der beim Kauf des Produkts vereinbart wurde. Wenn Sie unsicher sind, welcher Lizenztyp in Frage kommt, wenden Sie sich an den Händler, bei dem Sie die Software erworben haben.

4 Klicken Sie im Textfeld für die **Auswahl des Erwerbs- und Nutzungslandes** auf ▾, um das Land festzulegen, in dem die Software verwendet werden soll.

5 Lesen Sie die Lizenzvereinbarung sorgfältig durch. Wählen Sie anschließend eine der folgenden Optionen:

- Wenn Sie den Lizenzbestimmungen *zustimmen*, klicken Sie erst auf **Ich akzeptiere die Bedingungen des Lizenzvertrags** und dann auf **OK**, um fortzufahren.
- Wenn Sie den Bestimmungen *nicht zustimmen*, klicken Sie erst auf **Ich lehne die Bedingungen des Lizenzvertrags ab** und dann auf **Abbrechen**, um den Installationsvorgang abzubrechen.

6 Je nachdem, ob Sie die Software erstmals oder über eine frühere Version installieren, ist das Verfahren an dieser Stelle unterschiedlich:

- **Erstinstallation –** Wenn Sie die VirusScan Enterprise 7.1.0-Software zum ersten Mal oder erneut installieren (wenn Setup keine bereits installierte Version von NetShield, VirusScan oder VirusScan Enterprise findet), wird das Dialogfeld **Setup-Typ auswählen** angezeigt. Wechseln Sie zu *Starten der Installation* auf Seite 23, um weiterzumachen.
- **Frühere Version –** Wenn Sie die VirusScan Enterprise 7.1.0-Software über eine frühere Version von NetShield, VirusScan oder VirusScan Enterprise installieren, können Sie die Einstellungen für gespeicherte Tasks, benutzerdefinierte Erweiterungen und Ausschlusseinstellungen der bereits installierten Version beibehalten.

Das Dialogfeld **Frühere Version erkannt** wird angezeigt.



Abbildung 1-5. Frühere Version erkannt

- **Einstellungen beibehalten**: *Diese Option ist standardmäßig ausgewählt.* Deaktivieren Sie diese Option, wenn Sie die Einstellungen aus der früheren Version der Virenschutz-Software von McAfee nicht verwenden wollen.

  HINWEIS
  Wenn Sie **Einstellungen beibehalten** nicht aktivieren, werden die Einstellungen der zuvor installierten Software gelöscht.

- Klicken Sie auf **Weiter**, um fortzufahren.

Das Dialogfeld **Setup-Typ auswählen** wird angezeigt. Wechseln Sie zu *Starten der Installation* auf Seite 23, um weiterzumachen.

Starten der Installation

Die unter *Verwenden des Setupprogramms* auf Seite 18 beschriebenen Schritte müssen abgeschlossen sein, damit Sie mit einer standardmäßigen oder benutzerdefinierten Installation weitermachen können.

Wählen Sie im Dialogfeld **Setup-Typ auswählen** den gewünschten Setup-Typ:



Abbildung 1-6. Setup-Typ

- **Standard.** Installiert die Software mit allen Dienstprogrammen. Damit haben Sie die Möglichkeit, nach Viren zu suchen, Virusdefinitionsdateien (DAT) zu aktualisieren und Warnmeldungen zu senden. Diese Installation wird von McAfee Security für die meisten Umgebungen empfohlen.

  HINWEIS
  Mit der **Standardinstallation** ist es nicht möglich, die AutoUpdate-Repository-Liste zu importieren oder ein Benutzeroberflächenkennwort festzulegen. Um diese Features verwenden zu können, müssen Sie die Installation **Benutzerdefiniert** durchführen.

  Wechseln Sie zu *Standardinstallation* auf Seite 24, um mit der Installation weiterzumachen.

- **Benutzerdefiniert**: Damit können Sie selbst bestimmen, welche Features installiert werden sollen. Außerdem können Sie die AutoUpdate-Repository-Liste importieren, ein Benutzeroberflächenkennwort einrichten oder die Warnfunktion auf einer Arbeitsstation installieren.

  Wechseln Sie zu *Benutzerdefinierte Installation* auf Seite 26, um mit der Installation weiterzumachen.

Standardinstallation

Die unter *Verwenden des Setupprogramms* auf Seite 18 beschriebenen Schritte müssen abgeschlossen sein, bevor Sie mit einer standardmäßigen oder benutzerdefinierten Installation weitermachen können.

1 Wählen Sie im Dialogfeld **Setup-Typ auswählen** den Setup-Typ und den Installationspfad aus:

   a Wählen Sie **Standard**, falls diese Option nicht bereits ausgewählt ist.

   b Wählen Sie unter **Installieren in** den Installationspfad. Standardmäßig werden die VirusScan Enterprise-Programmdateien in folgendem Verzeichnis gespeichert:

   ```
   <Laufwerk>:\Programme\Network Associates\VirusScan
   ```

   Übernehmen Sie den Standardpfad, oder klicken Sie auf **Durchsuchen**, um einen anderen Pfad auszuwählen.

   c Klicken Sie auf **Speicherplatz**, um den Speicherplatzbedarf anzuzeigen. Klicken Sie dann auf **OK**, um zum Dialogfeld **Setup-Typ auswählen** zurückzukehren.

   d Klicken Sie auf **Weiter**, um fortzufahren.

   Das Dialogfeld **Bereit zur Installation** wird angezeigt.



Abbildung 1-7. Bereit zur Installation

2 Wenn die ausgewählten Installationseinstellungen korrekt sind, klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

> **HINWEIS**
> Klicken Sie auf **Zurück**, um die vorgenommenen Einstellungen zu überprüfen und zu ändern. Kehren Sie anschließend zum Dialogfeld **Bereit zur Installation** zurück, und klicken Sie auf **Installieren**.

Das Dialogfeld **McAfee VirusScan Enterprise wird installiert** zeigt den Status der Installation an.

Wenn der Setup-Vorgang abgeschlossen ist, wird das Dialogfeld **McAfee VirusScan Enterprise-Setup wurde erfolgreich abgeschlossen** angezeigt.



Abbildung 1-8. Setup erfolgreich abgeschlossen – Aktualisierungs- und Scan-Optionen

3 Nach Abschluss der Installation kann ein Aktualisierungs-Task oder ein Anforderungsscan-Task ausgeführt werden. Verwenden Sie eine Kombination folgender Optionen:

- **Jetzt aktualisieren**: *Diese Option ist standardmäßig ausgewählt.* Wenn der Aktualisierungs-Task bei Abschluss der Installation nicht gestartet werden soll, deaktivieren Sie diese Option.
- **Scannen auf Anforderung ausführen**: *Diese Option ist standardmäßig ausgewählt.* Wenn der standardmäßige Anforderungsscan-Task bei Abschluss der Installation nicht gestartet werden soll, deaktivieren Sie diese Option.

4 Klicken Sie nun auf **Fertig stellen**.

HINWEIS
Je nachdem, welche Optionen unter Schritt 3 ausgewählt wurden, führt das Programm nun das Aktualisierungsprogramm oder einen Anforderungsscan aus. Wenn Sie beide Optionen auswählen, wird zuerst der Aktualisierungs-Task und danach der Anforderungsscan-Task ausgeführt.

5 In einigen Situationen werden Sie aufgefordert, Ihren Computer neu zu starten. In diesem Fall wird das Dialogfeld **VirusScan-Setup** angezeigt.

Klicken Sie auf **Ja**, um jetzt neu zu starten. Wählen Sie **Nein**, um zu einem späteren Zeitpunkt neu zu starten.

Benutzerdefinierte Installation

Die unter *Verwenden des Setupprogramms* auf Seite 18 beschriebenen Schritte müssen abgeschlossen sein, bevor Sie mit einer benutzerdefinierten Installation weitermachen können.

1 Wählen Sie im Dialogfeld **Setup-Typ auswählen** den Setup-Typ und den Installationspfad aus:

   a Wählen Sie die Option **Benutzerdefiniert**.

   b Wählen Sie den Installationspfad unter **Installieren in**. Standardmäßig werden die VirusScan Enterprise-Programmdateien in folgendem Verzeichnis gespeichert:

   ```
   <Laufwerk>:\Programme\Network Associates\VirusScan
   ```

   Übernehmen Sie den Standardpfad, oder klicken Sie auf **Durchsuchen**, um einen anderen Pfad auszuwählen.

   c Klicken Sie auf **Speicherplatz**, um den Speicherplatzbedarf anzuzeigen. Klicken Sie dann auf **OK**, um wieder zum Dialogfeld **McAfee VirusScan Enterprise-Setup** zurückzukehren.

   d Klicken Sie auf **Weiter**, um fortzufahren.

Das Dialogfeld **Feature-Auswahl** wird angezeigt.

Abbildung 1-9. Feature-Auswahl

2 Wählen Sie unter **Wählen Sie die zu installierenden Features aus** die einzelnen Features aus, die installiert werden sollen.

- Wählen Sie spezifische Features aus. **Konsole** *ist standardmäßig ausgewählt.* Wenn Sie ein Feature auswählen, wird im rechten Fensterbereich jeweils eine kurze Beschreibung angezeigt.
- Außerdem können Sie im Dropdown-Menü für jedes markierte Feature eine entsprechende Aktion auswählen. Klicken Sie zum Anzeigen des Aktionsmenüs neben dem ausgewählten Feature auf ▾, und wählen Sie eine Aktion für dieses Feature aus.

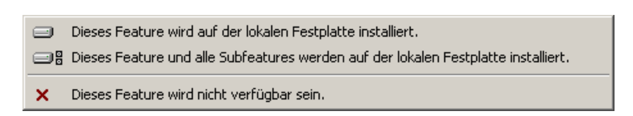


Abbildung 1-10. Aktionsoptionen zu einem Feature

Wählen Sie eine Kombination folgender Optionen:

- **Dieses Feature wird auf der lokalen Festplatte installiert:** Installiert das ausgewählte Feature auf dem Computer.
- **Dieses Feature und alle Subfeatures werden auf der lokalen Festplatte installiert:** Installiert das ausgewählte Feature und alle ihm untergeordneten Features. Wenn Sie z. B. **Konsole** auswählen, werden auch die Features **AutoUpdate**, **E-Mail-Scanner**, **Zugriffsscanner** und **Anforderungsscanner** installiert.
- **Dieses Feature wird nicht verfügbar sein:** Entfernt das ausgewählte Feature, wenn es bereits installiert ist.

e Übernehmen Sie den im Bereich **Installieren in** angegebenen Standardpfad oder klicken Sie auf **Durchsuchen**, um ein anderes Installationsverzeichnis festzulegen.

f Klicken Sie auf **Weiter**, um fortzufahren.

Das Dialogfeld **Warnungs-Manager installieren** wird angezeigt.



Abbildung 1-11. Warnungs-Manager installieren

HINWEIS
Der Installationsassistent erkennt, ob der Warnungs-Manager installiert ist. Ist das der Fall, so sind alle Optionen in diesem Dialogfeld deaktiviert.

3 Legen Sie fest, ob der Warnungs-Manager nach Abschluss der Installation von VirusScan Enterprise installiert werden soll:

a **Warnungs-Manager-Server installieren**: *Wenn es sich bei dem aktuellen Betriebssystem um einen Server handelt und der Warnungs-Manager im angegebenen Verzeichnis abgelegt und noch nicht installiert wurde, ist diese Option standardmäßig aktiviert.* Wenn der Warnungs-Manager nach Abschluss der Installation von VirusScan Enterprise nicht automatisch installiert werden soll, müssen Sie diese Option deaktivieren.

HINWEIS
Wenn Sie diese Option aktivieren, müssen die Warnungs-Manager-Dateien im unter **Warnungs-Manager-Installationsdateien** angezeigten Verzeichnis enthalten sein.

b **Warnungs-Manager-Installationsdateien**: Übernehmen Sie den Standardpfad, oder klicken Sie auf **Durchsuchen**, um ein anderes Verzeichnis auszuwählen.

WARNUNG
Wenn der Warnungs-Manager bei der ersten Installation von VirusScan Enterprise 7.1.0 nicht als Teil der benutzerdefinierten Installation installiert wird, kann er zu einem späteren Zeitpunkt nicht mit dem VirusScan Enterprise-Installationsprogramm installiert werden. Um den Warnungs-Manager nach der Installation von VirusScan Enterprise zu installieren, müssen Sie das eigenständige Installationsprogramm des Warnungs-Managers ausführen. Weitere Informationen finden Sie im *Warnungs-Manager 4.7-Produkthandbuch*.

c Klicken Sie auf **Weiter**, um fortzufahren.

Das Dialogfeld **Produktkonfiguration** wird angezeigt.



Abbildung 1-12. Produktkonfiguration

4 Wählen Sie im Dialogfeld **Produktkonfiguration** eine Kombination der folgenden Optionen und klicken Sie anschließend auf **Weiter**:

- **AutoUpdate-Repository-Liste importieren**: *Diese Option wird nur dann standardmäßig ausgewählt, wenn in der Installationsdatei (*.MSI*) eine Repository-Liste enthalten ist oder wenn die Befehlszeileneigenschaft (*CMASOURCEDIR*) auf einen neuen Speicherort festgelegt wurde, sodass auf die Datei* SITELIST.XML *verwiesen wird. Mithilfe von McAfee Installation Designer können Sie die Datei* SITELIST.XML *in die* .MSI*-Datei integrieren.* Wählen Sie diese Option aus, um die Repository-Liste aus dem angegebenen Verzeichnis zu importieren.

  - **AutoUpdate-Repository-Liste importieren**: Übernehmen Sie den Standardspeicherort, oder klicken Sie auf **Durchsuchen**, um ein anderes Verzeichnis auszuwählen.

HINWEIS
Wenn sich eine Repository-Liste im Installationsverzeichnis befindet, wird diese auch dann importiert, wenn Sie dies nicht explizit durch Auswählen der Option **AutoUpdate-Repository-Liste importieren** festlegen. Wenn eine Repository-Liste nicht importiert wird, führt AutoUpdate die Aktualisierungen unter Verwendung der Standardsite von Network Associates als Repository-Liste aus.

Weitere Informationen zur Repository-Liste finden Sie im *VirusScan Enterprise-Produkthandbuch* im Abschnitt *Aktualisieren*.

- **Zugriffsscanner nach Abschluss der Installation aktivieren**: *Diese Option ist standardmäßig ausgewählt.* Mit dieser Option wird der Zugriffsscanner nach Abschluss des Installationsvorgangs automatisch gestartet. Wenn Sie den Zugriffsscanner nach der Installation manuell starten möchten, müssen Sie diese Option deaktivieren.

5 Klicken Sie auf **Weiter**, um fortzufahren.

Das Dialogfeld **Sicherheitskonfiguration** wird angezeigt.

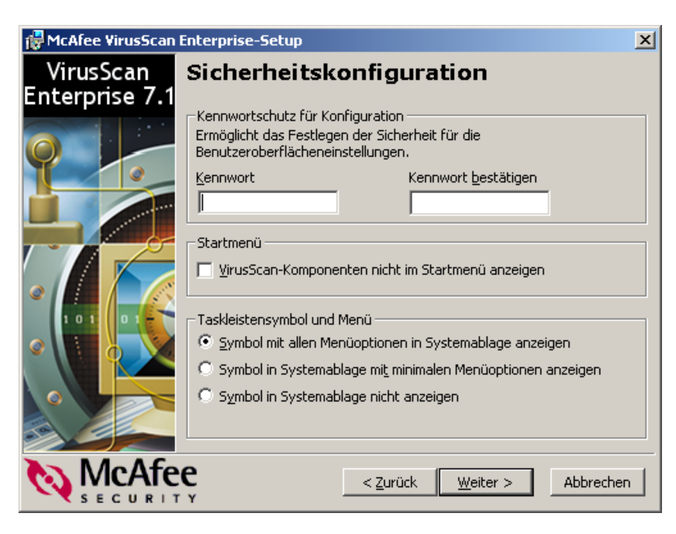


Abbildung 1-13. Sicherheitskonfiguration

6 Im Dialogfeld **Sicherheitskonfiguration** können Sie ein Benutzeroberflächenkennwort festlegen und bestimmen, welche Menüelemente den Benutzern angezeigt werden.

a Geben Sie im Bereich **Kennwortschutz für Konfiguration** das Benutzeroberflächenkennwort ein und bestätigen Sie es.

b Wenn Sie nicht möchten, dass die Menüoptionen für VirusScan im Startmenü angezeigt werden, wählen Sie im Bereich **Startmenü** die Option **VirusScan-Komponenten nicht im Startmenü anzeigen**.

c Wählen Sie im Bereich **Symbol in Systemablage und Menü** eine der folgenden Optionen aus:

- **Symbol mit allen Menüoptionen in Systemablage anzeigen**: *Diese Option ist standardmäßig ausgewählt.* Wenn nicht alle Menüoptionen für das Symbol in der Systemablage angezeigt werden sollen, muss die Option deaktiviert werden.
- **Symbol in Systemablage mit minimalen Menüoptionen anzeigen:** Den Benutzern werden in der Systemablage nur die Menüelemente **Info zu VirusScan Enterprise** und **Statistische Daten zum Scannen bei Zugriff** angezeigt. Alle anderen Menüoptionen werden für das Symbol in der Systemablage nicht angezeigt.
- **Symbol in Systemablage nicht anzeigen**: Benutzer haben keinen Zugriff auf die Systemablage der Statusleiste. Wenn Sie diese Option auswählen, wird in der Systemablage kein Symbol für das Menü angezeigt.

HINWEIS
Nach Abschluss der Installation können Sie den Kennwortschutz und die Optionen für Symbole in der Systemablage über die **VirusScan-Konsole** einrichten. Weitere Informationen finden Sie im *-Produkthandbuch* unter *VirusScan EnterpriseEinrichten von Benutzeroberflächenoptionen*.

d Klicken Sie auf **Weiter**, um fortzufahren.

Das Dialogfeld **Bereit zur Installation** wird angezeigt.



Abbildung 1-14. Bereit zur Installation

7 Wenn die ausgewählten Installationseinstellungen korrekt sind, klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

> **HINWEIS**
> Klicken Sie auf **Zurück**, um die vorgenommenen Einstellungen zu überprüfen und zu ändern. Kehren Sie anschließend zum Dialogfeld **Bereit zur Installation** zurück, und klicken Sie auf **Installieren**.

Das Dialogfeld **McAfee VirusScan Enterprise wird installiert** zeigt den Status der Installation an.

Wenn der Setup-Vorgang abgeschlossen ist, wird das Dialogfeld **McAfee VirusScan Enterprise-Setup wurde erfolgreich abgeschlossen** angezeigt.



Abbildung 1-15. Setup erfolgreich abgeschlossen – Aktualisierungs- und Scan-Optionen

8 Nach Abschluss der Installation kann ein Aktualisierungs-Task oder ein Anforderungsscan-Task ausgeführt werden. Verwenden Sie eine Kombination der folgenden Optionen:

- **Jetzt aktualisieren**: *Diese Option ist standardmäßig ausgewählt.* Wenn der Aktualisierungs-Task bei Abschluss der Installation nicht gestartet werden soll, deaktivieren Sie diese Option.

- **Scannen auf Anforderung ausführen**: *Diese Option ist standardmäßig ausgewählt.* Wenn der standardmäßige Anforderungsscan-Task bei Abschluss der Installation nicht gestartet werden soll, deaktivieren Sie diese Option.

9 Klicken Sie nun auf **Fertig stellen**.

HINWEIS
Je nachdem, welche Optionen unter Schritt 8 ausgewählt wurden, führt das Programm nun den Aktualisierungs-Task oder einen Anforderungsscan aus. Wenn Sie beide Optionen auswählen, wird zuerst der Aktualisierungs-Task und danach der Anforderungsscan-Task ausgeführt.

10 In einigen Situationen werden Sie aufgefordert, Ihren Computer neu zu starten. In diesem Fall wird das Dialogfeld **VirusScan-Setup** angezeigt.

Klicken Sie auf **Ja**, um jetzt neu zu starten. Wählen Sie **Nein**, um zu einem späteren Zeitpunkt neu zu starten.

Verwenden der Befehlszeile

Das VirusScan Enterprise-Setupprogramm wird als Microsoft Installer-Anwendung (.MSI) ausgeführt, wodurch Ihnen eine Vielzahl benutzerdefinierter Installationsoptionen zur Verfügung steht. Wenn Sie das Setup-Dienstprogramm über die Befehlszeile ausführen, können Sie die Installation so anpassen, dass sie Ihren Wünschen entsprechend ausgeführt wird und genau die von Ihnen angegebenen Produktfeatures installiert werden.

> **HINWEIS**
> Sie können das Setup-Programm über die Befehlszeile ausführen, um die VirusScan Enterprise-Software auf Ihrem *lokalen* Computer zu installieren, sofern Sie über Administratorrechte verfügen. Wenn Sie die Software auf einem *Remote*-Computer installieren möchten, müssen Sie ePolicy Orchestrator oder eine andere Software zur Produktbereitstellung verwenden. Weitere Informationen zur Verwendung von ePolicy Orchestrator zum Installieren der Programmdateien finden Sie im *VirusScan Enterprise-Konfigurationshandbuch*.

1. Klicken Sie auf **Start**, und wählen Sie anschließend **Ausführen**. Das Dialogfeld **Ausführen** wird angezeigt.

2. Geben Sie im Dialogfeld **Ausführen** den gewünschten Befehl ein, und klicken Sie anschließend auf **OK**.

   Die Setup-Befehlszeilensyntax lautet folgendermaßen:

   ```
   setup EIGENSCHAFT=WERT[,WERT] [/Option]
   ```

   Die Reihenfolge der Elemente dieser Syntax ist nicht festgelegt, eine Eigenschaft und deren Wert dürfen jedoch nicht voneinander getrennt werden. Die Syntax besteht aus:

   - **Dateiname –** Name der ausführbaren Datei: `setup.exe.`

   - **Optionen –** Vor jeder Option steht ein Schrägstrich (/). Zwischen Klein- und Großschreibung wird *nicht* unterschieden. In den weiter unten in diesem Handbuch beschriebenen Installationsszenarien werden einige der verfügbaren Optionen beschrieben.

   - **Eigenschaften–** Alle Eigenschaften, die Sie zum Anpassen der Installation verwenden möchten.

     Jede Eigenschaft besteht aus:

     - einem Namen, der vollständig in Großbuchstaben angegeben werden muss.

     - einem Gleichheitszeichen (=).

- einem oder mehreren durch Kommas getrennten Werten. Die meisten Eigenschaftenwerte müssen ebenfalls vollständig in Großbuchstaben angegeben werden, bei einigen Werten (z. B. True und False) muss jedoch Gemischtschreibung verwendet werden. Microsoft Installer lässt eine Vielzahl von Eigenschaften zu, mit denen Sie die Installation anpassen können. Weitere Informationen zu diesen Eigenschaften finden Sie in der Dokumentation für Microsoft Installer. Diese zusätzlichen Eigenschaften können Sie speziell für die Installation der VirusScan Enterprise-Software verwenden:
- ADDLOCAL. Installiert bestimmte Features auf dem lokalen Computer.
- INSTALLDIR. Gibt an, welches Installationsverzeichnis verwendet werden soll. Der Wert besteht aus dem Verzeichnispfad.
- PRESERVESETTINGS. Gibt an, ob Setup die Konfigurationsoptionen beibehalten soll, die in vorherigen Zugriffsscanner-Installationen verwendet wurden. Standardmäßig lautet der Wert dieser Eigenschaft True.
- REBOOT. Gibt an, ob Setup den Computer neu starten soll. Sie können den Neustart des Computers bei Bedarf erzwingen oder verhindern.
- REMOVE. Entfernt ein oder mehrere Programmfeatures. Sie können ein bestimmtes Feature angeben oder den Wert ALL verwenden, um alle Features zu entfernen. Wenn Sie diese Eigenschaft mit der Eigenschaft ADDLOCAL kombinieren, können Sie alle Features mit Ausnahme von einem oder zwei bestimmten Features installieren.
- REMOVEINCOMPATIBLESOFTWARE. Entfernt die Virenschutzsoftware eines anderen Anbieters, um Konflikte mit dieser Version von VirusScan Enterprise zu verhindern. Standardmäßig lautet der Wert dieser Eigenschaft True.

In den folgenden Abschnitten werden einige übliche Szenarien beschrieben, in denen die Befehlszeilenoptionen zum Ausführen von benutzerdefinierten Installationen verwendet werden.

Installation im Hintergrund

Verwenden Sie die Befehlszeilenoptionen, um eine Installation der VirusScan Enterprise-Software auf allen Netzwerkknoten so einzurichten, dass der Benutzer nur wenige oder gar keine Schritte ausführen muss. Bei der Installation im Hintergrund werden die üblichen Assistentenfenster nicht angezeigt und der Benutzer kann keine Konfigurationsoptionen auswählen. Stattdessen werden diese Angaben von Ihnen vorkonfiguriert, und das Setup wird auf allen Zielcomputern im Hintergrund ausgeführt. Sie können die VirusScan Enterprise-Software mit oder ohne Wissen des Endbenutzers auf einem beliebigen nicht besetzten Computer installieren, sofern Sie über alle erforderlichen Administratorrechte verfügen.

Beispiel: `setup/q`:

- Verwenden Sie `/q`, wenn die Installation im Hintergrund ausgeführt werden soll.
- Andere, teilweise im Hintergrund ausgeführte Installationsmethoden sind:

`/qb`	Während der Installation wird ein kleiner Fortschrittsbalken und eine Schaltfläche zum Abbrechen angezeigt.
`/q+`	Es wird ein Dialogfeld mit der Meldung angezeigt, ob die Installation erfolgreich abgeschlossen wurde oder fehlgeschlagen ist.
`/qb+`	Sowohl der Fortschrittsbalken als auch das Abschlussdialogfeld werden angezeigt.
`/qf`	Zeigt während der Installation den Fortschritt und eine Schaltfläche zum Abbrechen an.

Wenn der Installationsfortschritt in einer Protokolldatei erfasst werden soll, fügen Sie der Setup-Befehlszeile diese Option und diesen Parameter hinzu:

```
/l*v "c:\temp\log.txt"
```

`c:\temp\log.txt` kann hier ein beliebiges Verzeichnis und ein beliebiger Dateiname sein, in dem Sie die Protokolldatei erstellen möchten. Diese Option erfasst alle Installationsaktivitäten, einschließlich aller kopierten Dateien, aller hinzugefügten Registrierungsschlüssel und aller Änderungen von .INI-Dateien.

Ersetzen Sie das Sternchen (*) in dem Befehlszeilenbeispiel durch einen oder mehrere dieser Parameter, um die Art der Daten einzuschränken, die in der Protokolldatei erfasst werden:

`i`	Statusmeldungen
`w`	nicht schwerwiegende Warnungen
`e`	alle Fehlermeldungen
`a`	Start von Aktionen
`r`	aktionsspezifische Einträge
`u`	Benutzeranforderungen
`c`	anfängliche Benutzeroberflächenparameter
`m`	nicht genügend Arbeitsspeicher oder schwerwiegender Abbruch
`o`	nicht genügend Speicherplatz
`p`	Terminaleigenschaften
`+`	Daten an vorhandene Datei anfügen
`!`	alle Zeilen in das Protokoll schreiben

Installieren in einem benutzerdefinierten Verzeichnis

Wenn die VirusScan Enterprise-Software in einem benutzerdefinierten Verzeichnis installiert werden soll, fügen Sie in der Befehlszeile die Eigenschaft INSTALLDIR ein. Fügen Sie zu der Eigenschaft anschließend einen Wert für das zu verwendende Verzeichnis hinzu. Wenn die VirusScan Enterprise-Software beispielsweise im Verzeichnis C:\Meine Antivirus-Software installiert werden soll, müssen Sie die folgende Zeile an der Eingabeaufforderung eingeben:

setup INSTALLDIR= "c:\Meine Antivirus-Software" /q

Anführungszeichen sind nur erforderlich, wenn der Name des Zielverzeichnisses Leerzeichen enthält. Sie können auch die Option /q verwenden, um die Installation im Hintergrund auszuführen.

Auswählen bestimmter zu installierender Features

Wenn Sie das Setup über die Befehlszeile ausführen, um bestimmte Programm-Features zu installieren, installiert das Dienstprogramm diese Features entsprechend einer bereits vorhandenen Hierarchie. Wenn Sie beispielsweise nur die VirusScan Enterprise-Shell-Erweiterungen installieren, weiß Setup demnach, dass die -ANWENDUNG scan32.exeVirusScan Enterprise installiert sein muss, um die Erweiterungen verwenden zu können. Daher werden sowohl diese Datei als auch alle dazugehörigen Dateien installiert.

Um die zu installierenden Features anzugeben, müssen Sie bestimmte Feature-Namen als Befehlszeilenparameter hinzufügen. Sie können folgende Feature-Namen über die Befehlszeile angeben:

Feature-Name	Beschreibung
AutoUpdate	Das AutoUpdate-Dienstprogramm
Console	Die VirusScan Enterprise-Konsole
EmailScan	Der E-Mail-Scanner und die E-Mail-Scan-Erweiterung
OnAccessScanner	Der Zugriffsscanner
OnDemandScanner	Der Anforderungsscanner
ShellExtentions	Erweiterungen, die Kontextmenüfunktionen hinzufügen, mit denen Sie einzelne Dateien scannen können

HINWEIS
Sie können einzelne Features angeben oder die Eigenschaft ALLE verwenden, um alle Features zu installieren.

- Geben Sie zum Verwenden dieser Feature-Namen in einer Befehlszeile das Ziel und den Namen des Features genau so an, wie er in der Tabelle angegeben ist.

  Geben Sie beispielsweise zum Hinzufügen der VirusScan Enterprise-Anwendung zu dem lokalen System die folgende Zeile an der Eingabeaufforderung ein:

  ```
  setup.exe ADDLOCAL=ALL/q
  ```

- Wenn Sie mehrere Features installieren wollen, benutzen Sie ein Komma, um die Werte voneinander zu trennen. Geben Sie beispielsweise zum gleichzeitigen Hinzufügen des Anforderungs- und Zugriffsscanners an der Eingabeaufforderung die folgende Zeile ein:

  ```
  setup.exe ADDLOCAL=OnAccessScanner,OnDemandScanner/q
  ```

- Für eine vollständige Installation geben Sie an der Eingabeaufforderung folgende Zeile ein:

  ```
  setup.exe ADDLOCAL=ALL/q
  ```

- Um sämtliche VirusScan Enterprise-Komponenten zu entfernen, geben Sie an der Eingabeaufforderung folgende Zeile ein:

  ```
  setup.exe REMOVE=ALL/q
  ```

- Um sämtliche Features außer einem zu installieren, beispielsweise alle ohne das Feature E-Mail-Scanner, geben Sie an der Eingabeaufforderung folgende Zeile ein:

  ```
  setup.exe ADDLOCAL=ALL REMOVE=EmailScan/q
  ```

- Sie können auch verschiedene Features für eine nicht im Hintergrund auszuführende Installation auswählen. Wenn Sie beispielsweise die in einigen der Beispiele gezeigte Option `/q` weglassen, zeigt das Assistentenfenster für die benutzerdefinierte Installation (siehe *Benutzerdefinierte Installation* auf Seite 26) nur die Features an, die Sie als zur Installation verfügbar angegeben haben. Wenn Sie dieselben Beispiele verwenden, um einen Featuresatz für die Installation festzulegen, installiert Setup nur die während einer **Standard**installation festgelegten Features.

Installationseigenschaften anpassen

Bei der Installation über die Befehlszeile können Sie den Installationsvorgang mithilfe von bestimmten Eigenschaften anpassen. Sie können hier folgende Eigenschaften anpassen:

Befehlszeileneigenschaft	Funktion
ALERTMANAGERSOURCEDIR	Stellt den Standardquellpfad des Warnungs-Managers ein. Der Standardpfad ist \AMG. Sie können diese Einstellung auch in der Datei SETUP.INI vornehmen.
CMASOURCEDIR	Stellt den Quellpfad für SITELIST.XML ein. Der Standardpfad lautet: %TEMP%\NAITemp.
ENABLEONACCESSSCANNER	False = Ein False-Wert kann nicht eingestellt werden. True = Aktiviert den Zugriffsscanner nach Abschluss der Installation. Dies ist die Standardeinstellung. **Hinweis:** Wenn Sie den Zugriffsscanner nicht aktivieren möchten, setzen Sie die Eigenschaft auf "". Das bedeutet: ENABLEONACCESSSCANNER="", eine leere Zeichenfolge.
EXTRADATSOURCEDIR	Legt den Verzeichnispfad für EXTRA.DAT fest. Während der Installation wird die Datei EXTRA.DAT in das Verzeichnis kopiert, in dem sich die Moduldateien befinden.
FORCEAMSINSTALL	True = Warnungs-Manager installieren, wenn vorhanden.
INSTALLDIR	Legt das Standardinstallationsverzeichnis fest.
INSTALLCHECKPOINT	False = Integration von Check Point SCV wird nicht installiert. True = Integration von Check Point SCV wird installiert.

Befehlszeileneigenschaft	Funktion
LOCKDOWNVIURUSSCANSHORTCUTS	False = Ein False-Wert kann nicht eingestellt werden. True = Zeigt keine Verknüpfungen im Startmenü an. **Hinweis:** Wenn die Verknüpfungen installiert werden sollen, setzen Sie die Eigenschaft auf "". Das bedeutet: LOCKDOWNVIURUSSCANSHORTCUTS ="", eine leere Zeichenfolge. Dies ist die Standardeinstellung.
PRESERVESETTINGS	Beibehalten der Einstellungen beim Upgrade von NetShield 4.5, VirusScan 4.5.1 oder VirusScan Enterprise 7.0. False = Ein False-Wert kann nicht eingestellt werden. True = Einstellungen beibehalten. Dies ist die Standardeinstellung. **Hinweis:** Wenn Sie die Einstellungen nicht beibehalten möchten, setzen Sie die Eigenschaft auf "". Das bedeutet: PRESERVESETTINGS="", eine leere Zeichenfolge.
RUNAUTOUPDATE	False = Ein False-Wert kann nicht eingestellt werden. True = Führt nach Abschluss der Installation AutoUpdate aus. Dies ist die Standardeinstellung. **Hinweis:** Wenn AutoUpdate nach Abschluss der Installation nicht ausgeführt werden soll, setzen Sie die Eigenschaft auf "". Das bedeutet: RUNAUTOUPDATE="", eine leere Zeichenfolge.
RUNONDEMANDSCAN	False = Ein False-Wert kann nicht eingestellt werden. True = Scannt alle lokalen Laufwerke nach Abschluss der Installation. Dies ist die Standardeinstellung. **Hinweis:** Wenn der Anforderungsscanner nach Abschluss der Installation nicht ausgeführt werden soll, setzen Sie die Eigenschaft auf "". Das bedeutet: RUNONDEMANDSCAN="", eine leere Zeichenfolge.

Befehlszeileneigenschaft	Funktion
RUNAUTOUPDATESILENTLY	False = Ein False-Wert kann nicht eingestellt werden. True = Führt nach Abschluss der Installation eine automatische Aktualisierung aus. Der Standardwert ist eine leere Zeichenfolge. **Hinweis:** Wenn nach Abschluss der Installation keine automatische Aktualisierung ausgeführt werden soll, setzen Sie die Eigenschaft auf "". Das bedeutet: RUNAUTOUPDATESILENTLY="", eine leere Zeichenfolge.
RUNONDEMANDSCANSILENTLY	False = Ein False-Wert kann nicht eingestellt werden. True = Führt nach Abschluss der Installation einen automatischen Anforderungsscan aus. Der Standardwert ist eine leere Zeichenfolge. **Hinweis:** Wenn nach Abschluss der Installation kein automatischer Anforderungsscan ausgeführt werden soll, setzen Sie die Eigenschaft auf "". Das bedeutet: RUNONDEMANDSCANSILENTLY="", eine leere Zeichenfolge.

Einrichten von Neustartoptionen

Sie können einen Neustart bei Bedarf erzwingen oder aber verhindern, dass der Zielcomputer bei der Installation neu gestartet wird. Fügen Sie der Befehlszeile dazu die Eigenschaft REBOOT hinzu.

- Mit `REBOOT=F` wird der Neustart bei Bedarf erzwungen.
- Mit `REBOOT=R` wird der Neustart verhindert.

Wenn Sie zunächst den Windows Installer-Dienst auf einem Zielcomputer installieren müssen, müssen Sie einen Neustart durchführen, unabhängig davon, ob Sie den Neustart aus anderen Gründen erzwingen oder verhindern möchten. Das Setup wird fortgeführt, nachdem MSI den Neustart erzwungen hat. Anschließend werden die Optionen verwendet, die Sie angegeben haben, um festzulegen, ob der Neustart nach der Installation erzwungen oder verhindert werden soll.

```
setup REBOOT=R /q
```

In diesem Beispiel wird eine Installation im Hintergrund und kein Systemneustart ausgeführt.

Entfernen nicht kompatibler Software

Setup entfernt standardmäßig nicht kompatible Software während einer Installation im Hintergrund. Als nicht kompatible Software gelten dabei alle Produkte anderer Anbieter. Wenn nicht kompatible Software nicht entfernt werden soll, müssen Sie der Befehlszeile die Eigenschaft REMOVEINCOMPATIBLESOFTWARE mit dem Wert False hinzufügen:

```
setup REMOVEINCOMPATIBLESOFTWARE=False
```

Beibehalten von Einstellungen

Setup behält standardmäßig die Einstellungen vorheriger VirusScan- und NetShield-Installationen bei. Um die neue VirusScan Enterprise-Version ohne die vorherigen Einstellungen zu installieren, müssen Sie in der Befehlszeile die Eigenschaft PRESERVESETTINGS mit einem auf eine leere Zeichenfolge gesetzten Wert hinzufügen:

```
setup PRESERVESETTINGS=""
```

Ausführen des Setups aus einem Anmeldeskript

Um die VirusScan Enterprise-Software bei jedem Start der Zielcomputer zu installieren, können Sie zu dem Anmeldeskript eine Setup-Befehlszeile hinzufügen und jede Logik einbeziehen, die Ihrer Meinung nach für die einmalige Ausführung der Installation erforderlich ist, wie beispielsweise die Suche nach dem Standardprogrammverzeichnis für VirusScan Enterprise. Die Befehlszeile muss alle Optionen und Eigenschaften enthalten, die zur Steuerung der Installation verwendet werden sollen.

- Wenn Sie dazu ein Anmeldeskript verwenden möchten, müssen Sie außerdem das VirusScan Enterprise-Installationspaket in ein lokales Verzeichnis auf dem Zielcomputer kopieren bzw. dorthin "abrufen". Die *-Software kann mit einem Anmeldeskript* nichtVirusScan Enterprise von einem anderen Standort im Netzwerk aus installiert werden. Verwenden Sie zum Installieren der VirusScan Enterprise-Software von einem anderen Standort im Netzwerk die Verwaltungssoftware McAfee ePolicy Orchestrator.

Installierte Dateien

Bei der VirusScan Enterprise-Installation werden die Dateien im Installationspfad in folgenden Verzeichnissen installiert:

- *VirusScan Ordner* auf Seite 44.
- *Res09-Ordner* auf Seite 45.
- *Modulordner* auf Seite 45.

HINWEIS
Der Installationspfad wird während der Installation bestimmt. Der Standard-Installationspfad lautet:

```
<Laufwerk>:\Programme\Network Associates\VirusScan
```

VirusScan Ordner

Diese Dateien werden im Installationsverzeichnis, VirusScan-Ordner, installiert:

- AdsLokUU.Dll
- dssdata.h
- DSSDATA.INI
- emconfig.exe
- ftcfg.dll
- Ftl.dll
- license.txt
- logparser.exe
- McAVDetect.DLL
- mcavscv.dll
- mcconsol.exe
- Mcshield.exe
- mcupdate.exe
- MERTool.url
- midutil.dll
- NaEventU.Dll
- naiann.dll
- naiavf5x.cat
- naiavf5x.inf
- naiavf5x.sys
- naiavfin.exe
- NaiEvent.dll
- nailite.dll
- NaKrnlU.Dll
- nautilu.dll
- NTClient.dll
- Packing.lst
- pireg.exe
- readme.txt
- scan32.exe
- ScanEmal.Dll
- scncfg32.exe
- scnstat.exe
- SDATPACK.LST
- shcfg32.exe
- shext.dll
- shstat.exe
- shutil.dll
- SVCPWD.exe
- VSPlugin.dll
- VSTskMgr.exe
- vsupdate.dll
- Weitere beibehaltene Einstellungen

Res09-Ordner

Diese Dateien werden im Installationsverzeichnis im Res09-Ordner installiert:

- FtCfgRC.dll
- McConsol.DLL
- McShield.DLL
- mcupdate.DLL
- NaEvtRes.Dll
- NaUtlRes.Dll
- Product.DLL
- Scan32.DLL
- ScnCfg32.DLL
- ScnStat.DLL
- SEmalRes.Dll
- ShCfg32.DLL
- shextres.dll
- ShStat.DLL
- ShUtilRc.DLL
- vse.chm
- VSTskMgr.DLL
- amg.chm (sofern der Warnungs-Manager installiert ist)

Modulordner

Diese Dateien werden im Modul-Ordner installiert, der sich im folgenden Pfad befindet:

```
<Laufwerk>:\Program Files\Common Files\Network Associates\
```

- AvParam.dll
- clean.dat
- EXTRA.DAT
- license.dat
- mcscan32.dll
- MCTOOL.EXE
- messages.dat
- names.dat
- scan.dat
- scan.exe
- SCAN86.EXE
- SignLic.txt

Überprüfen der Installation

Nach der Installation kann die Software das System nach infizierten Dateien durchsuchen. Sie können überprüfen, ob die Software richtig installiert ist und korrekt nach Viren suchen kann, indem Sie einen Test implementieren, der von EICAR (European Institute for Computer Anti-Virus Research), einem Zusammenschluss von Antivirus-Softwareherstellern entwickelt wurde, um ihren Kunden eine Möglichkeit zu bieten, beliebige Antivirus-Software-Installationen zu überprüfen.

So überprüfen Sie die Installation:

1 Geben Sie mit einem Standard-Texteditor, wie Notepad, die folgende Zeichenfolge *in einer einzigen Zeile und ohne Leerzeichen oder Zeilenumbrüche ein*:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$
H+H*
```

2 Speichern Sie die Datei unter dem Namen EICAR.COM. Die Dateigröße beträgt 68 Byte. Merken Sie sich das Verzeichnis, in dem die Datei gespeichert wurde.

3 Starten Sie das Programm.

- Testen Sie den Anforderungsscanner, indem Sie einen Anforderungsscan-Task erstellen, der das Verzeichnis überprüft, in dem EICAR.COM gespeichert wurde. Während der Überprüfung der Datei meldet der Scanner, dass die Testdatei EICAR gefunden wurde.

- Um den Zugriffsscanner zu überprüfen, stellen Sie sicher, dass er für das Scannen von auf den Computer geschriebenen und aus dem Computer gelesenen Dateien konfiguriert wurde. Weitere Informationen finden Sie im *-Produkthandbuch* unter *VirusScan EnterpriseKonfigurieren des Zugriffsscanners*. Suchen Sie als Nächstes die Datei EICAR.COM, und versuchen Sie, sie in ein anderes Verzeichnis zu kopieren oder zu verschieben. Bei der Prüfung der Datei meldet der Scanner, dass die Testdatei EICAR gefunden wurde.

  HINWEIS
  Diese Datei ist *kein Virus* – sie kann sich nicht ausbreiten, andere Dateien infizieren oder Ihr System beschädigen. Löschen Sie die Datei nach dem Überprüfen Ihrer Installation, um zu verhindern, dass andere Benutzer mit der Warnmeldung konfrontiert werden.

Ändern von VirusScan Enterprise

Mithilfe des Setup-Dienstprogramms können Sie die VirusScan Enterprise-Programmdateien ändern oder reparieren.

Diese Themen sind in diesem Abschnitt enthalten:

- *Starten des Setupprogramms*.
- *Ändern von Programm-Features* auf Seite 49.
- *Neuinstallieren oder Reparieren von Programmdateien* auf Seite 52.

Starten des Setupprogramms

1 Klicken Sie auf **Start**, und wählen Sie anschließend **Ausführen**. Das Dialogfeld **Ausführen** wird angezeigt.

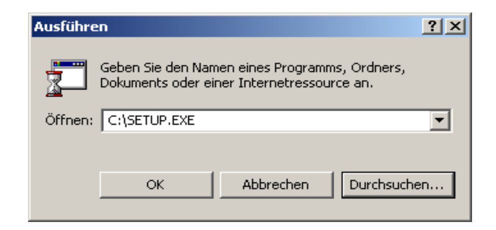


Abbildung 1-16. Ausführen

2 Geben Sie in das angegebene Textfeld den Befehl `<X>:\SETUP.EXE` ein, und klicken Sie auf **OK**.

`<X>:` steht dabei für den Laufwerksbuchstaben des CD-ROM-Laufwerks bzw. für den Pfad zu dem Ordner, der die entpackten Programmdateien enthält. Um nach der entsprechenden Datei auf der Festplatte oder CD-ROM zu suchen, klicken Sie auf **Durchsuchen**. Wenn Sie die Software von einer Total Virus Defense-CD installieren, müssen Sie außerdem angeben, in welchem Ordner die VirusScan Enterprise-Software gespeichert ist.

Das Dialogfeld **Programmwartung** wird angezeigt.

Abbildung 1-17. Programmwartung

3 Wählen Sie die auszuführende Programmwartungs-Aktivität aus.

- **Ändern**. *Diese Option ist standardmäßig ausgewählt.* Ändern Sie die zu installierenden Programm-Features. Diese Option verwendet zum Ändern der installierten Features das Dialogfeld **Feature-Auswahl**.

  Lesen Sie zum Abschließen der Änderungen den Abschnitt *Ändern von Programm-Features* auf Seite 49.

- **Reparieren**. Wählen Sie diese Option, um die Programmdateien neu zu installieren oder zu reparieren.

  Lesen Sie zum Abschließen der Neuinstallation oder der Reparatur den Abschnitt *Neuinstallieren oder Reparieren von Programmdateien* auf Seite 52.

- **Remove**. Wählen Sie diese Option, um die Programmdateien zu entfernen.

  Weitere Informationen zum Entfernen von Programmdateien finden Sie unter *Entfernen der Software* auf Seite 55.

Ändern von Programm-Features

1 Wählen Sie im Dialogfeld **Programmwartung** die Option **Ändern**. Klicken Sie anschließend auf **Weiter**.

Das Dialogfeld **Feature-Auswahl** wird angezeigt.

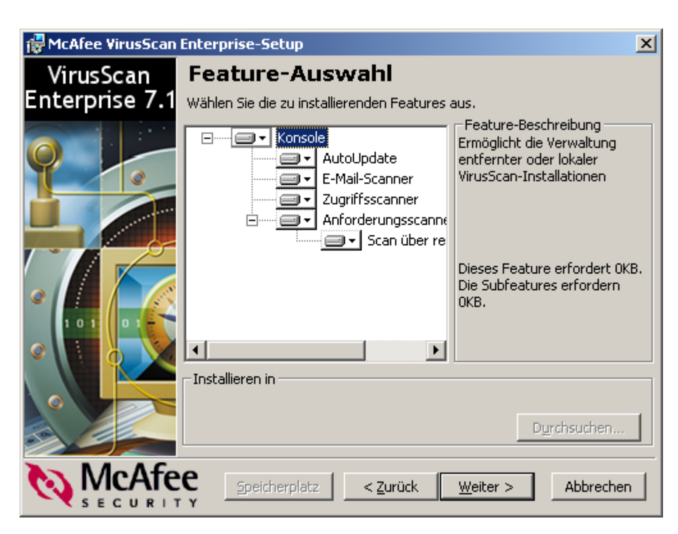


Abbildung 1-18. Feature-Auswahl – Ändern

2 Unter **Wählen Sie die zu installierenden Features aus** wählen Sie die einzelnen Features aus, die installiert werden sollen.

- Wählen Sie spezifische Features aus. **Konsole** *ist standardmäßig ausgewählt.* Wenn Sie ein Feature auswählen, wird im rechten Fensterbereich jeweils eine kurze Beschreibung angezeigt.
- Außerdem können Sie im Dropdown-Menü für jedes markierte Feature eine entsprechende Aktion auswählen. Klicken Sie zum Anzeigen des Aktionsmenüs neben dem ausgewählten Feature auf ▾, und wählen Sie eine Aktion für dieses Feature aus.

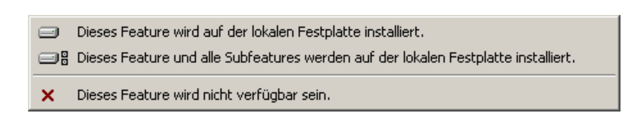


Abbildung 1-19. Aktionsoptionen zu einem Feature

Wählen Sie eine Kombination der folgenden Optionen:

- **Dieses Feature wird auf der lokalen Festplatte installiert:** Installiert das ausgewählte Feature auf dem Computer.
- **Dieses Feature und alle Subfeatures werden auf der lokalen Festplatte installiert:** Installiert das ausgewählte Feature und alle ihm untergeordneten Features. Wenn Sie beispielsweise **Konsole** auswählen, werden auch die Features **AutoUpdate**, **E-Mail-Scanner**, **Zugriffsscanner** und **Anforderungsscanner** installiert.
- **Dieses Feature wird nicht verfügbar sein:** Entfernt das ausgewählte Feature, wenn es bereits installiert ist.

HINWEIS
Die Optionen **Installieren in** und **Speicherplatz** sind deaktiviert. Um den Installationspfad zu ändern, müssen Sie das Produkt zunächst entfernen und dann in dem gewünschten Pfad neu installieren.

3 Klicken Sie auf **Weiter**, um fortzufahren.

Das Dialogfeld **Produktkonfiguration** wird angezeigt.



Abbildung 1-20. Produktkonfiguration – Ändern

4 Wählen Sie im Dialogfeld **Produktkonfiguration**, ob Sie am Ende der Installation den Zugriffsscanner aktivieren wollen.

- **Zugriffsscanner nach Abschluss der Installation aktivieren**: *Diese Option ist standardmäßig ausgewählt.* Mit dieser Option wird der Zugriffsscanner nach Abschluss des Installationsvorgangs automatisch gestartet. Wenn Sie den Zugriffsscanner nach der Installation manuell starten möchten, müssen Sie diese Option deaktivieren.

  HINWEIS
  Die Option **AutoUpdate-Repository-Liste importieren** ist deaktiviert. Informationen zum Importieren der Repository-Liste finden Sie im -*Produkthandbuch* im Abschnitt *VirusScan EnterpriseAktualisieren*.

5 Klicken Sie auf **Weiter**, um das Dialogfeld **Bereit zur Installation** zu öffnen.

6 Wenn die ausgewählten Installationseinstellungen korrekt sind, klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

  HINWEIS
  Klicken Sie auf **Zurück**, um die vorgenommenen Einstellungen zu überprüfen und zu ändern. Kehren Sie anschließend zum Dialogfeld **Bereit zur Installation** zurück, und klicken Sie auf **Installieren**.

7 Wenn das Setup erfolgreich abgeschlossen wurde, klicken Sie auf **Fertig stellen**.

Neuinstallieren oder Reparieren von Programmdateien

1 Wählen Sie im Dialogfeld **Programmwartung** die Option **Reparieren**. Klicken Sie anschließend auf **Weiter**.

Das Dialogfeld **Produkt neu installieren oder reparieren** wird angezeigt.



Abbildung 1-21. Produkt neu installieren oder reparieren

2 Wählen Sie eine der folgenden Wartungsoptionen:

- **Neuinstallation von VirusScan Enterprise**. *Diese Option ist standardmäßig ausgewählt.* Mit der Option werden die Programmdateien, Registrierungsschlüssel und Verknüpfungen neu installiert.
- **Fehlende oder beschädigte Dateien erkennen und reparieren**: Mit dieser Option werden fehlende und beschädigte Dateien erkannt und repariert.
  - **Registrierungsschlüssel neu schreiben**.

WARNUNG
Wenn Sie Dateien manuell entfernen oder umbenennen, kann das Reparatur-Feature möglicherweise nicht ausgeführt werden. Ausführliche Anweisungen zum Reparieren von Dateien, die entfernt oder umbenannt wurden, finden Sie im Anhang *Fehlerbehebung* des *VirusScan Enterprise-Produkthandbuchs*.

WARNUNG

Weder das Feature **Neuinstallation von VirusScan Enterprise** noch das Feature **Fehlende oder beschädigte Dateien erkennen und reparieren** unterstützen die Neuinstallation oder Reparatur von Aktualisierungskomponenten. Wenn eine AutoUpdate-Datei entfernt oder beschädigt wird, muss die Aktualisierungskomponente erst entfernt und dann neu installiert werden.

Um die Aktualisierungskomponente mit VirusScan Enterprise zu entfernen, verwenden Sie das Setupprogramm oder entfernen Sie die Programmdateien über die Befehlszeile. Weitere Informationen finden Sie unter *Entfernen der Software* auf Seite 55.

Wenn die Aktualisierungskomponente in einer ePolicyOrchestrator-Umgebung bereitgestellt wurde, können Sie die Programmdateien entfernen. Die Aktualisierungskomponente wird dann von ePolicyOrchestrator erneut installiert. Weitere Informationen finden Sie im *Produkthandbuch für ePolicy Orchestrator*.

3 Klicken Sie auf **Installieren**.

Wenn der Setup-Vorgang abgeschlossen ist, wird das Dialogfeld **McAfee VirusScan Enterprise-Setup wurde erfolgreich abgeschlossen** angezeigt.



Abbildung 1-22. Setup erfolgreich abgeschlossen – Aktualisierungs- und Scan-Optionen

4 Ein Aktualisierungs-Task oder ein Anforderungsscan-Task kann sofort nach Abschluss der Installation ausgeführt werden. Verwenden Sie eine Kombination der folgenden Optionen:

- **Jetzt aktualisieren**: *Diese Option ist standardmäßig ausgewählt.* Wenn der AutoUpdate-Task bei Abschluss der Installation nicht gestartet werden soll, deaktivieren Sie diese Option.
- **Scannen auf Anforderung ausführen**: *Diese Option ist standardmäßig ausgewählt.* Wenn der standardmäßige Anforderungsscan-Task bei Abschluss der Installation nicht gestartet werden soll, deaktivieren Sie diese Option.

5 Klicken Sie nun auf **Fertig stellen**.

> **HINWEIS**
> Je nachdem, welche Optionen unter Schritt 3 ausgewählt wurden, führt das Programm nun das Aktualisierungsprogramm oder einen Anforderungsscan aus. Wenn Sie beide Optionen auswählen, wird zuerst der Aktualisierungs-Task und danach der Anforderungsscan-Task ausgeführt.

6 In einigen Situationen werden Sie aufgefordert, Ihren Computer neu zu starten. In diesem Fall wird das Dialogfeld **VirusScan-Setup** angezeigt.

Klicken Sie auf **Ja**, um jetzt neu zu starten. Wählen Sie **Nein**, um zu einem späteren Zeitpunkt neu zu starten.

Entfernen der Software 2

Sie können die VirusScan Enterprise-Programmdateien auf eine der folgenden Arten entfernen:

- *Verwenden des Setup-Dienstprogramms* auf Seite 56.
- *Verwenden der Befehlszeilenoptionen* auf Seite 59.
- *Verwenden des Dienstprogramms "Software"* auf Seite 59.

Verwenden des Setup-Dienstprogramms

Auf dem Computer, von dem das Programm entfernt werden soll:

1 Öffnen Sie das Dialogfeld **McAfee VirusScan Enterprise-Setup**. Verwenden Sie dazu eine der folgenden Methoden:

Wenn sich Ihre Kopie der Software auf der Produkt-CD befindet:

a Legen Sie die CD in das CD-ROM-Laufwerk ein.

b Klicken Sie im Dialogfeld **Willkommen** auf **Installation**.

Wenn Sie die Software heruntergeladen haben:

a Klicken Sie auf **Start**, und wählen Sie anschließend **Ausführen**. Das Dialogfeld **Ausführen** wird angezeigt.

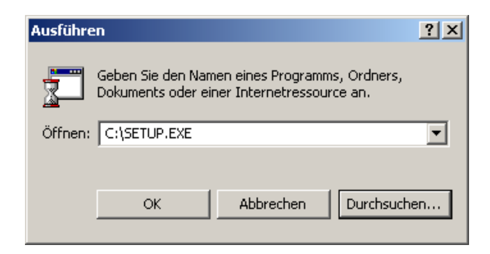


Abbildung 2-1. Ausführen

b Geben Sie in das Textfeld den Befehl `<X>:\SETUP.EXE` ein, und klicken Sie auf **OK**.

`<X>` steht dabei für den Laufwerksbuchstaben des CD-ROM-Laufwerks bzw. für den Pfad zu dem Ordner, der die entpackten Programmdateien enthält. Um nach der entsprechenden Datei auf der Festplatte oder CD-ROM zu suchen, klicken Sie auf **Durchsuchen**. Wenn Sie die Software von einer Produktsuite-CD installieren, müssen Sie außerdem angeben, in welchem Ordner die gewünschte Software gespeichert ist.

Das Dialogfeld **Programmwartung** wird angezeigt.



Abbildung 2-2. Programmwartung

2 Wählen Sie **Entfernen**, und klicken Sie auf **Weiter**.

Das Dialogfeld **McAfee VirusScan Enterprise entfernen** wird angezeigt.



Abbildung 2-3. VirusScan Enterprise entfernen

3 Klicken Sie auf **Entfernen**, um mit dem Löschvorgang zu beginnen.

4 Wenn das Setup erfolgreich abgeschlossen wurde, klicken Sie auf **Fertig stellen**.

Das Deinstallationsprogramm erkennt, ob noch Dateien oder Verzeichnisse übrig geblieben sind. Hierbei handelt es sich beispielsweise um Dateien oder Verzeichnisse, Protokolldateien oder andere Dateien oder Verzeichnisse, die vom Benutzer hinzugefügt wurden und nicht bei der ursprünglichen Installation von VirusScan Enterprise installiert wurden.



Abbildung 2-4. Verbleibende Dateien entfernen

Wenn die Programmdateien entfernt wurden, verbleiben zwei Dateien im Protokollverzeichnis %TEMP%\NAI . Diese Dateien werden zu Fehlerbehebungszwecken verwendet:

- VSEUninst.log
- VSEInst.log

5 Klicken Sie auf **Ja**, um die verbleibenden Dateien zu entfernen. Wenn die verbleibenden Dateien nicht entfernt werden sollen, klicken Sie auf **Nein**.

6 Starten Sie Ihren Computer nach Abschluss der Deinstallation neu.

WARNUNG
Es wird dringend empfohlen, den Computer nach dem Entfernen der Dateien neu zu starten. Der Neustart sollte vor einer Neuinstallation durchgeführt werden.

Wenn Sie Dateien über SETUP.EXE oder die Befehlszeile entfernen, werden möglicherweise einige Dateien oder gestoppte Dienste nicht entfernt. Wenn Sie zum Beispiel das VirusScan Enterprise-Produkt entfernen, während die Dienste Network Associates-Task-Manager oder Network Associates McShield gestoppt sind, werden diese Dienste nicht entfernt. Durch einen Neustart nach dem Entfernen von Dateien wird sichergestellt, dass alle Dateien und Dienste vor einer Neuinstallation entfernt werden.

Verwenden der Befehlszeilenoptionen

1 Öffnen Sie die Windows-Eingabeaufforderung mithilfe einer der folgenden Methoden:

   - Wählen Sie im Menü **Start** die Option **Eingabeaufforderung**.
   - Wählen Sie im Menü **Start** die Option **Ausführen**.

2 Geben Sie in der Eingabeaufforderung oder im Dialogfeld **Ausführen** folgende Zeichenfolge ein:

```
<X>:\SETUP.EXE/x
```

   <X> steht dabei für den Laufwerksbuchstaben des CD-ROM-Laufwerks bzw. für den Pfad zu dem Ordner, der die entpackten Programmdateien enthält. Um nach der entsprechenden Datei auf der Festplatte oder CD-ROM zu suchen, klicken Sie auf **Durchsuchen**. Wenn Sie die Software von einer Produktsuite-CD installieren, müssen Sie außerdem angeben, in welchem Ordner die gewünschte Software gespeichert ist.

3 Starten Sie Ihren Computer nach Abschluss der Deinstallation neu.

WARNUNG
Es wird dringend empfohlen, den Computer nach dem Entfernen der Dateien neu zu starten. Der Neustart sollte vor einer Neuinstallation durchgeführt werden.

Wenn Sie Dateien über SETUP.EXE oder die Befehlszeile entfernen, werden möglicherweise einige Dateien oder gestoppte Dienste nicht entfernt. Wenn Sie zum Beispiel das VirusScan Enterprise-Produkt entfernen, während die Dienste Network Associates-Task-Manager oder Network Associates McShield gestoppt sind, werden diese Dienste nicht entfernt. Durch einen Neustart nach dem Entfernen von Dateien wird sichergestellt, dass alle Dateien und Dienste vor einer Neuinstallation entfernt werden.

Verwenden des Dienstprogramms "Software"

Zum Aufrufen des Dienstprogramms **Software** in der Windows-Systemsteuerung wählen Sie **Start** | **Einstellungen** | **Systemsteuerung** | **Software**.

Netopsystems FEAD Optimizer



Die VirusScan Enterprise 7.1.0-Installationsdatei (.MSI) wurde mithilfe der Netopsystems FEAD Optimizer-Technologie optimiert. Diese Technologie verringert die Größe des Installationspakets.

Diese Themen sind in diesem Abschnitt enthalten:

- Befehlszeileneigenschaften und -optionen
- Standardwerte für optimierte Datei

Befehlszeileneigenschaften und -optionen

Wenn Sie die Datei SETUP.EXE von der Befehlszeile aus ausführen, können Befehlszeileneigenschaften und -optionen zusammen mit einer optimierten Datei verwendet werden, um den Neuaufbau der Zieldatei benutzerdefiniert anzupassen.

Die Syntax lautet:

setup.exe [<Optionen>...]

Die Optionen werden definiert als:

<Optionen> = < Netopsystems-Optionen> | <VirusScan EnterpriseOptionen>

Die VirusScan Enterprise-Optionen sind Parameter, die an das VirusScan Enterprise-Setup-Dienstprogramm weitergeben werden. Zum Beispiel:

setup.exe -s -nos_d INSTALLDIR="c:\abc def" /L

setup.exe NOCDI=TRUE -nos_o"d:\temp" -nos_s REBOOT=A

Diese Befehlszeileneigenschaften oder -optionen können mit einer optimierten Datei verwendet werden.

Befehlszeileneigenschaft oder -optionen	Funktion
-nos_ne	Keine Ausführung — Extrahiert die Setup-Datei aus SETUP.EXE, führt die Datei SETUP.EXE jedoch nicht aus oder löscht die Setup-Dateien.
-nos_nd	Kein Löschen — Setup-Dateien werden nach Ausführen von SETUP.EXE nicht gelöscht. Wenn die Option nos_-ne nicht vorhanden ist, wird die nos_-nd-Option übergangen.
-nos_d	Löschen – Die Setup-Dateien werden nach dem Ausführen von SETUP.EXE gelöscht. Wenn die Option nos_-ne auch vorhanden ist, wird die nos_-d-Option übergangen.
-nos_s	Hintergrundmodus – Die Setup-Dateien werden im Hintergrundmodus installiert. (Installiert automatisch bei /s, /S,-s, -S, /q, /Q, -q, -Q).
-nos_o"<Pfad>"	Ausgabeordner – Der Ordner, in den die Setup-Dateien extrahiert werden sollen.

Standardwerte für optimierte Datei

Die Standardaktionen lauten wie folgt:

Aktion	Standard
Ausführung	Ja
Löschen	Ja
im Hintergrund	Nein
Ausgabeordner	%TEMP%\McAfee VirusScan Enterprise 7

Check Point konfigurieren



Die VirusScan Enterprise-Software wurde für die Integration von Check Point VPN-1/FireWall-1-SCV erweitert.

Nun ist das McAfee Check Point Secure Configuration Verification-(SCV)-Plugin (MCAVSCV.DLL) verfügbar, das die beiden Produkte integriert. Bei diesem Plugin handelt es sich um eine Dynamic Link Library, die der *Check Point*™ VPN-*1/FireWall-1*® SCV-*(Secure Configuration Verification)-Spezifizierung* vom November 2001 entspricht. Diese Spezifizierung finden Sie auf der Web-Site der Open Platform for Security (OPSEC):

http://www.opsec.com

Wenn Check Point installiert und aktiv ist, kann das Produkt konfiguriert werden, um einen Zugriff auf der Grundlage des geschützten Status von VirusScan Enterprise auf das System zu erlauben oder zu blockieren.

Diese Themen sind in diesem Abschnitt enthalten:

Client-Computer-Installation

Wenn Sie die VirusScan Enterprise 7.1.0-Software installieren, werden im Installationsverzeichnis folgende Dateien für die Verwendung mit Check Point installiert:

- MCAVSCV.DLL
- MCAVDETECT.DLL

Das Standardinstallationsverzeichnis ist:

```
Program Files\Network Associates\VirusScan
```

Wenn der Check Point SecuRemote™-Registry-Eintrag vorhanden ist, wird das SCV-Plugin mit Check Point VPN-1 und/oder Firewall-1 registriert.

Wenn das Check Point-Produkt erst im Anschluss an VirusScan Enterprise installiert wird, muss VirusScan Enterprise 7.1.0 erneut installiert werden.

Um das Plugin MCAVSCV.DLL zu registrieren, führen Sie folgende Schritte durch:

1. Brechen Sie den SecureClient-Dienst ab.
2. Installieren Sie VirusScan Enterprise 7.1.0.
3. Starten Sie den SecureClient-Dienst, nachdem VirusScan Enterprise das SCV-Plugin registriert hat.

Nach der Registrierung kann das Plugin MCAVSCV.DLL von VPN-1 oder Firewall-1 genutzt werden, um den VirusScan Enterprise-Schutz zu erzwingen, sofern der Check Point-Administrator folgende Maßnahmen getroffen hat:

- Aktivierung der SCV-Prüfung.
- Hinzufügen des McAfee SCV-Abschnitts auf dem Sicherheitsrichtlinienserver für das Check Point-System in der LOVAL.SCV.

Administratorkonfiguration

Der Check Point-Administrator kann die Richtliniendatei (LOCAL.SCV) auf dem Check Point-Server bearbeiten, um die Anforderungen des VirusScan Enterprise-Schutzes für VPN-1 und/oder Firewall-1 zu verändern.
Dies ist ein Beispielabschnitt einer LOCAL.SCV-Datei, die eine Richtlinie für ein MCAVSCV.DLL-Plugin enthält, das im VirusScan Enterprise-Installationspaket enthalten ist.

Sie finden den SCV-Editor unter:

http://www.checkpoint.com/techsupport/downloadsng/utilities.html

Eine Erläuterung der Syntax für den LOCAL.SCV finden Sie in der Dokumentation zu Check Point VPN-1, die Sie mit Ihrem Check Point-Produkt erhalten haben.

Dies ist ein Beispielabschnitt einer local.scv-Datei, die eine Richtlinie für das mcavscv.dll-Plugin enthält, das im Installationspaket von VirusScan Enterprise enthalten ist.

```
: (mcavscv
 :type (plugin)
 :parameters (
     :product (VSE)
     :minimum_product (7.1)
     :minimum_product (4260)
     :minimum_dat (4260)
     :dat_age_max_days (30)
     :begin_admin (admin)
     :send_log (alert)
     :mismatchmessage
     McAffee VirusScan Enterprise ist nicht aktiv oder ist
     veraltet, bitte führen Sie AutoUpdate aus oder aktivieren
     Sie den Zugriffsscanner.
     :end (admin)
 )
)
```

Der Check Point-Administrator kann die Schutzanforderungen von VirusScan Enterprise für VPN-1 und/oder Firewall-1 wie folgt ändern.

- Der Name des Plugins ist *mcavscv* und muss in Kleinbuchstaben angegeben werden. Wir setzen voraus, dass der Administrator der Check Point-Sicherheitsrichtlinien mit der Konfiguration der SCV-Richtlinien für Check Point-Produkte vertraut ist.
- *:product* ist optional und muss für VirusScan Enterprise *VSE* sein. Es sind zurzeit keine anderen Produktwerte implementiert. Die Schutzprüfung von VirusScan Enterprise liefert *nicht geschützt* zurück, wenn VirusScan Enterprise nicht auf dem System installiert ist, das diese SCV-Prüfung ausführt.
- *:minimum_product* ist optional und wird ignoriert, wenn es nicht in der SCV-Datei enthalten ist. Gültige Werte sind zurzeit *7.0* und *7.1*. Die Schutzprüfung von VirusScan Enterprise liefert *nicht geschützt* zurück, wenn die installierte Version des Produkts (zurzeit immer *VSE*) unter dem Wert liegt, der auf dem System angegeben wurde, das diese SCV-Prüfung durchführt.
- *:minimum_engine* ist optional und lautet, wenn es nicht spezifiziert wird, *4260*. Die Schutzprüfung von VirusScan Enterprise liefert *nicht geschützt* zurück, wenn die installierte Modul-Version niedriger ist als die, die auf dem System angegeben wurde, das diese SCV-Prüfung durchführt.
- *:minimum_dat* ist optional und wird ignoriert, wenn keine Angabe vorgenommen wird. Die Schutzprüfung von VirusScan Enterprise liefert *nicht geschützt* zurück, wenn die installierte DAT-Version niedriger ist als der Wert, der auf dem System angegeben wurde, das diese SCV-Prüfung durchführt.
- *:dat_age_max_days* ist optional und lautet, wenn es nicht spezifiziert wird, *31*. Die Schutzprüfung von VirusScan Enterprise liefert *nicht geschützt* zurück, wenn die installierte DAT älter ist als die, die auf dem System angegeben wurde, das diese SCV-Prüfung durchführt.
- *:mismatchmessage* spezifiziert die Nachricht, die angezeigt wird, wenn die VirusScan Enterprise-Schutzprüfung *nicht geschützt* ergibt. Der Check Point-Administrator konfiguriert, wo diese Nachrichten protokolliert werden, oder ob sie dem Benutzer angezeigt werden.

Die VirusScan Enterprise-Schutzprüfung liefert den Status *geschützt* an Check Point VPN-1 oder Firewall-1, wenn alle oben genannten Prüfungen abgeschlossen (oder ignoriert) wurden und folgende Bedingungen vorliegen:

- Es wurde kein Status *nicht geschützt* angezeigt.
- Der VirusScan Enterprise-Zugriffsscanner läuft und ist aktiv.

Andernfalls wird der Status *nicht geschützt* zurückgeliefert.

Index